WANG

Wang Systems Networking

VS Network Control and Monitoring Guide

Wang Systems Networking

VS Network Control and Monitoring Guide

2nd Edition — July 1988

715-0164A

WANG LABORATORIES, INC.
ONE INDUSTRIAL AVENUE, LOWELL, MA 01851 TEL. (508) 459-5000, TELEX 172108

Disclaimer of Warranties and Limitation of Liabilities

The staff of Wang Laboratories, Inc., has taken due care in preparing this manual. However, nothing contained herein modifies or alters in any way the standard terms and conditions of the Wang purchase, lease, or license agreement by which the product was acquired, nor increases in any way Wang's liability to the customer. In no event shall Wang or its subsidiaries be liable for incidental or consequential damages in connection with or arising from the use of the product, the accompanying manual, or any related materials.

Software Notice

All Wang Program Products (software) are licensed to customers in accordance with the terms and conditions of the Wang Standard Software License. No title or ownership of Wang software is transferred, and any use of the software beyond the terms of the aforesaid license, without the written authorization of Wang, is prohibited.

Warning

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

CONTENTS

CONTENTS (continued)

CHAPTER 3 MONITORING APPLICATIONS AND SESSIONS

CHAPTER 4 MONITORING SYSTEMS AND ROUTES

CHAPTER 5 CNS DIAGNOSTICS

CHAPTER 8 USING THE WSN CONFIGURATION REPORTER

FIGURES

FIGURES (continued)

TABLES

TABLES (continued)

PREFACE

This book is intended for network and local system administrators who control and monitor the communications components in a Wang Systems Networking environment. It describes the VS tools that allow you to perform these control and monitoring functions.

Chapter 1 introduces communications control and monitoring on a VS system. The chapter describes the Communications Network Services (CNS) control and monitoring program CNS Manager, the standard VS Operator's Console, the Wang Band Monitor, and the WSN Configuration Reporter. Chapter 1 also shows you how to access the CNS Manager and the Event Inquiry Facility.

Chapter 2 describes the steps for using the CNS Manager to control and monitor WSN transports that are defined on your local VS.

Chapter 3 shows you how to monitor applications and sessions with the CNS Manager.

Chapter 4 shows you how to monitor the CNS routes over which data is transmitted between systems.

Chapter 5 describes the diagnostic programs that can be accessed by the CNS Manager.

Chapter 6 describes the network control features on the standard VS Operator's Console.

Chapter 7 describes the Wang Band Monitor, and how you can display status information from the Cable Interface Units that are attached to each system on the WangNet Wang Band cable.

Chapter 8 describes the WSN Configuration Reporter. The WSN Configuration Reporter allows you to generate reports from the information contained in your network's current configuration file.

Appendix A lists the logger subsystem IDs that you can specify in the Event Inquiry Facility. Appendix B describes the messages associated with Communications Network Services (CNS). Appendix C lists and defines the Operator's Console error messages associated with the File Transfer Manager (FTM) and the Session Manager. Appendix D explains the light emitting diode status lights for the Cable Interface Units (CIUs), VS Telecommunications Controllers (VS-TCs), Multi-Line Telecommunications Controller (MLTC), and modems. It also describes some of the problems you may encounter with your system's network communications, and it offers possible responses to those problems.

Those who use this manual should have access to the following Wang documents:

- *VS Network Configuration Guide* (715-0165)
- *VS System Administrator's Reference* (715-0420)
- *VS System Operator's Reference* (800-1102-08)
- *VS System Operator's Guide* (715-0418A)
- *VS System Utilities Reference* (715-0421A)
- *Network User Guide for VS Systems* (800-1316D)
- *Virtual Terminal Interface User's Guide* (700-8668)

CHAPTER 1
INTRODUCTION

OVERVIEW

This chapter introduces the VS facilities that allow you to control and monitor network communications activity in a Wang Systems Networking (WSN) environment. When a VS system is equipped with the appropriate components, it can control a set of hardware and software elements that allow it to communicate with other systems in the network.

There are four VS tools that allow you to control or monitor the network activity that takes place when your local system is communicating with other computers in the network. They are

- Communications Network Services Manager
- VS Operator's Console
- Wang Band Monitor
- WSN Configuration Reporter

Note: *The term "local system" refers to the system onto which you are logged. The system could be the system to which your workstation is physically attached, or a remote system onto which you are logged through use of the WSN VS Terminal Emulation service (i.e., remote logon).*

Communications Network Services Manager

The Communications Network Services Manager allows you to monitor and control the WSN routing component, called Communications Network Services (CNS). CNS provides common access for WSN applications and services across the network. The CNS Manager provides you with information concerning CNS activity on the local system, and allows you to perform the following functions:

- Control and monitor the WSN transports that are defined on your local VS. Transports are responsible for the movement of data between adjacent nodes within a WSN framework. Transports are able to detect transmission errors, retransmit data, and report problems to other network nodes. The CNS Manager Transports function displays the current status of all transports that have been defined through WSNEDIT, as well as the number of bytes and messages sent and received via CNS, the number of incoming messages rejected via CNS, the base and total costs for the transport, and the reactivation timer. This function also allows you to enable or disable transports and to modify Base cost and Reactivation timer values.

- Monitor the applications and sessions that are currently attached to CNS. A session is established when an application (such as File Transfer) on your local system is communicating with another application on a remote system. The CNS Manager Apps/Sessions function allows you to display all applications that are currently attached to CNS, as well as the number of inbound and outbound sessions that are currently active involving each application.

  The CNS Manager Monitor Application screen displays the ID of the application's user and the number of messages and bytes that the application has sent or received. The screen also displays the current number of sessions the application has initiated, the current number of sessions that applications on remote systems have initiated with the application, and the maximum number of inboumd sessions the application can support.

  The CNS Manager Monitor Session screen displays the status of an active session that you select. The screen displays the session ID, indicates whether the session was initiated by the local system or a remote system, gives the name and local application session ID of the application that is the local session partner, and specifies the number of data messages, bytes, acknowledgments, and credits sent and received during the session.

- Control and monitor the CNS routing activity between your local system and a destination system. When you send information to a destination system, CNS uses the routing information that you specified in WSNEDIT, as well as CNS-generated routing records (stored in memory), to establish the least cost path to the destination system/area.

The CNS Manager Monitor Systems/Routes function displays the status of the routes that were defined through WSNEDIT. It indicates whether or not destination systems have been initialized, and displays the Path cost of each route and the status of the transports that connect the local system and adjacent systems. It is recommended that you read the CNS Routing Overview in Chapter 2 of the *VS Network Configuration Guide* before you access the Monitor Systems/Routes function for the first time.

- Access and attach diagnostic programs to CNS. These programs allow you to determine the rate of data transfer across a line, the amount of time between the sending and receiving of a message, the accuracy of data transfer, the path that a data message will take from the local system to a destination system, and the number of systems that the local system can contact in the network.

  When you select a diagnostic program and then specify the appropriate parameters, the program attaches to CNS and initiates a session with a peer application, known as PASSTEST, at the specified destination system. PASSTEST is automatically submitted to run in background at the destination system.

  The diagnostic programs include

  Throughput Test (THRUTEST) -- Measures the effective user data throughput in bits/second between two systems.

  Propagation Delay Test (PROPTEST) -- Measures the propagation delay for data transfer between two systems. The propagation delay is the amount of time it takes for a message transmitted to a remote system to return to the originating system.

  Synchronous Send/Receive Test (SYNCTEST) -- Verifies the accuracy of data transferred between two systems.

  Connect Test (CONECTST) -- Determines whether the remote systems running CNS can be reached.

  Path Trace -- Traces the path that a data message takes from the local system to a destination system.

  CNS Trace -- Sets specified trace points within CNS.

- Monitor local system network communications activity with the Event Inquiry Facility. The Event Inquiry Facility allows you to view real-time messages that are associated with communications activity on your local system (e.g., reasons for failed attempts to communicate). The messages are stored in chronological order in a daily log file. You can also use the Event Inquiry Facility to display and print the log information associated with a specific date and time.

VS Operator's Console

The VS Operator's Console contains functions that allow you to control and monitor network communications activity. These control and monitoring functions include

Transmit Queue -- Allows you to control and monitor the files that are awaiting transmission from your local system to remote systems

Retrieve Queue -- Allows you to control and monitor the files that are awaiting retrieval from remote systems

Interactive Tasks -- Allows you to control and monitor the programs that are currently being used by the workstations in your network

Telecommunications -- Allows you to control and monitor links, devices, systems, and services

Workstations -- Allows you to control and monitor the workstations on your local system

Chapter 6 describes the functions on the VS Operator's Console.

Wang Band Monitor

The Wang Band Monitor allows you to display status information from the Cable Interface Units (CIUs) that are attached to each system in your network. A CIU (internal or external) is the hardware device that connects a VS system to the WangNet cable. If you are using Wang Band transports to communicate with other systems in your network, you can use the Wang Band Monitor to poll or request data from each CIU. This data includes

- A listing of all systems on Wang Band, an indication of whether or not a system was able to respond to a Wang Band Monitor poll, and the number of virtual circuits that are currently active on each successfully polled system

- The circuit status of a selected system on the Wang Band, including the number of virtual circuits that are supported by the CIU type (internal or external), and the current state of each virtual circuit

- The CIU traffic statistics and error counts (unit status) of a selected system on the Wang Band

Chapter 7 describes the Wang Band Monitor.

WSN Configuration Reporter

The WSN Configuration Reporter allows you to generate reports from the information contained in your network's current configuration file. When you create and print these reports, you can easily view the network configuration information without accessing the WSNEDIT utility. You can refer to the reports when you are planning for network expansion or when you want to make adjustments to your current configuration for more efficient network operation.

GETTING STARTED

This section describes the network functions that you must perform before starting your network.

Specifying Your Logger Volume

Before starting your network, you must specify a VS volume for the logging of network messages. These messages can be CNS messages, as well as messages that are generated by WSN applications and services (e.g., File Transfer, VS Terminal Emulation). In a non-DMF environment, you specify this volume with the procedure named LOGCNTRL.

To run the LOGCNTRL procedure, perform the following steps:

1. Log on to the VS. The VS Command Processor screen appears.

2. Press PF1. The Run screen appears.

3. Type LOGCNTRL in the PROGRAM field on the screen. Specify @SYSCOM@ in the LIBRARY field, and press ENTER. At the prompt, enter the name of the VS volume that you want to use for the logging of network messages, and press ENTER.

When you start your network background tasks with the procedure named WSNSTART (described in the next section), the logging task (LOGTSK) creates a library named @LOG@ on your designated VS volume. When the CNS task is running, all network activity messages during a given day are saved in a daily log file in the @LOG@ library. The LOGTSK program names each daily log file in the format, *Lyymmdd*, where *L* indicates log file, *yy* indicates the year, *mm* indicates the month, and *dd* indicates the day.

When two or more VS systems are communicating over the network, you can use the Event Inquiry Facility to view network messages as they are sent. The Event Inquiry Facility is described in this chapter.

Running WSNSTART and WSNSTOP

WSNSTART submits background tasks for all installed networking software. After using the LOGCNTRL program to specify your network logger volume, run the procedure WSNSTART to submit the appropriate background tasks. The tasks include the log task (LOGTSK), the CNS task (CNSTSK), and other installed applications that depend on CNS.

To run the WSNSTART procedure, perform the following steps:

1. Log on to the VS. The VS Command Processor screen appears.

2. Press PF1. The Run screen appears.

3. Type WSNSTART in the PROGRAM field on the screen. Press ENTER.

WSNSTOP stops the background tasks. If you want to change your logger volume while the network is running, run WSNSTOP to stop the CNS task, the logger task, and all installed applications that are running in background. Use the LOGCNTRL procedure to specify your logger volume, and run the WSNSTART procedure to restart your network.

Note: *Exercise caution when running WSNSTOP. If you need to re-IPL your local VS, you must first run WSNSTOP to halt the CNS task and the log task. Since the WSNSTOP procedure ends prior to the actual halting of the log task, you must be certain that all network tasks have halted before IPLing the VS. Otherwise, network tasks may remain open. This condition results from the unsuccessful completion of these network tasks prior to the IPL.*

ACCESSING THE CNS MANAGER

The CNS Manager uses intertask messages to communicate with the CNS task on a VS system. CNS is a layered software architecture that provides applications with a method of network access. CNS control software queries each layer for information on that particular layer's activity. The CNS Manager provides an interface to the CNS control software, allowing users to monitor this information.

CNS architecture is summarized in the *VS Network Configuration Guide*.

To access the CNS Manager, perform the following steps:

1. Log on to the VS. The VS Command Processor screen appears.

2. Press PF1. The Run screen appears.

3. Type CNSMGR in the PROGRAM field on the screen. Press ENTER. The procedure CNSMGR is created in the system library on the system volume during the installation of WSN VS NETCORE. If CNSMGR does not reside in the system library on the system volume, enter the names of the appropriate library and volume in the LIBRARY and VOLUME fields. The CNS Manager Summary Status screen appears (Figure 1-1).

The CNS Manager Summary Status screen provides usage statistics on current CNS activity. This information includes the status of the CNS task, the CNS revision level, the time(s) and date(s) that both CNS and CNS Manager were started, system and user identification, message summary totals, and CNS utilization totals. From the CNS Manager Summary Status screen, you can access the detailed status information associated with transports, applications and sessions, and routes. You can also access the CNS Manager diagnostic programs.

Chapters 2 through 5 tell you how to use the detailed status information to control and monitor the CNS activity associated with the functions on the CNS Summary Status screen.

```
                        Wang Laboratories, Inc.                    12 May
                    Distributed Management Facility                08:40

                        - CNS Manager Summary Status -     (c) Copr. Wang 1988

Manager Status:     ACTIVE                  CNS Status:  ACTIVE
Manager Rev:        01.00.00                CNS Rev:     04.01.00
Manager Started:    01/10/88 at 14:00       CNS Started: 01/01/88 at 14:00
System:             UPTOWN                      by User: WPS

Message Summary     Totals                                Maximum  Current
Received:             1000          CNS Buffers:             11       11
Sent:                  900          Applications:           249        2
Passed Through:        100          Sessions:               256        5

                    Number of Areas: 15    Number of Systems: 34
                          Number of Transports: 42

            Press (ENTER) to update status or (17) for Event Inquiry
(2) Stop CNS     (6) Systems/Routes (10) Diagnostics                (16) Exit
(5) Transports   (7) Apps/Sessions  (11) Update 060 secs
```

Figure 1-1. CNS Manager Summary Status Screen

The CNS Manager Summary Status screen displays the general status of CNS. The general status includes information on the number of transports defined, the number of applications attached to CNS, and the number of sessions currently established. It includes the number of messages sent and received, as well as the number of messages that have been passed through the local system. There is also information on CNS buffers, the number of areas, and the number of systems in the network.

You can start and stop the CNS task from the CNS Manager Summary Status screen.

The fields that appear on the CNS Manager Summary Status screen are as follows:

Manager Status -- The current status of the CNS Manager background task. If you do not have the Distributed Management Facility installed on your local system, the status is always ACTIVE.

CNS Status -- The current status of CNS. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE you can stop CNS by pressing PF2 from the CNS Manager Summary Status screen.

INACTIVE -- If the CNS status is INACTIVE you can start CNS by pressing PF1 from the CNS Manager Summary Status screen.

TIMEOUT -- The CNS Manager has sent a message to CNS but no response has been received.

Manager Rev -- The revision of the CNS Manager software you are currently running on the local system.

CNS Rev -- The revision of the CNS software you are currently running on the local system.

Manager Started -- The time and date that the CNS Manager was started.

CNS Started by User -- The time and date when CNS was started, and the logon ID of the user who started CNS.

System -- The system from which you are obtaining statistics.

Messages Received -- The number of messages the system has received since CNS was last started.

Messages Sent -- The number of messages sent by CNS since CNS was last started.

Messages Passed Through -- The number of messages that have passed through the system since CNS was last started. These messages were routed on behalf of other systems.

CNS Buffers (Maximum) -- Whenever a module within CNS attempts to send a message to another module, the sending module must allocate a buffer or memory space to format the message. When the message is received, the receiving module can retain that buffer space to send a reply or release the buffer space back to a common pool. If a module attempts to send a message and no buffer space is available, the module must wait until space is available. This field displays the maximum number of buffers that have been concurrently allocated. (One buffer represents the amount of memory needed to format a message.)

CNS Buffers (Current) -- The number of buffers that are available.

Applications (Maximum) -- The maximum number of applications that can attach to CNS.

Applications (Current) -- The current number of applications attached to CNS.

Sessions (Maximum) -- The maximum number of sessions that CNS can support.

Sessions (Current) -- The current number of active sessions.

Number of Areas -- The number of areas defined in the network directory. These areas are defined through WSNEDIT.

Number of Systems -- The number of systems defined in the network directory. These systems are defined through WSNEDIT.

Number of Transports -- The maximum number of transports supported by CNS, as defined in WSNEDIT.

Functions on the CNS Manager Summary Status Screen

Table 1-1 lists the functions that are available on the CNS Manager Summary Status screen.

Table 1-1. CNS Manager Summary Status Screen Functions

When You Press	You Can
PF1 (Start CNS)	Start CNS. This key is only active if CNS is inactive. When you press PF1, the screen displays the message "WARNING: CNS will be activated, (ENTER) to continue or (16) to return."
PF2 (Stop CNS)	Stop CNS. This key is active only if CNS is active. When you press PF2, the screen displays the message "WARNING: CNS will be terminated, (ENTER) to continue or (16) to return".
PF5 (Transports)	Go to the Select CNS Transports for Management screen.
PF6 (Systems/Routes)	Go to the Monitor Systems/Routes screen.
PF7 (Apps/Sessions)	Go to the Select Application or Session to Monitor screen.
PF10 (Diagnostics)	Go to the CNS Diagnostics menu.
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field are 0 - 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Exit)	Return to the program from which you accessed the CNS Manager Summary Status screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
ENTER	Request an immediate status update from CNS.

STARTING AND STOPPING CNS

You can independently start and stop the CNS task by pressing PF1 from the CNS Manager Summary Status screen. This function does not affect the other non-CNS related network tasks that are currently running in background. If the CNS task is not running, press PF1 (Start CNS) from the CNS Manager Summary Status screen to start CNS. If the log task program (LOGTSK) is not running when you start CNS, then CNS starts LOGTSK. LOGTSK is the background program that creates and maintains daily log files. A daily log file contains a chronological listing of network messages that are logged by the LOGTSK program on your local system. The Event Inquiry Facility, described later in this chapter, allows you to monitor these messages.

When the CNS status is ACTIVE, you can press PF2 (Stop CNS) to stop the CNS task. You may find it necessary to stop CNS if you detect network problems that are associated with CNS. Stopping the CNS task does not stop the other background tasks that are currently running on your VS. You can modify the network configuration file while the network tasks are running. However, most changes do not take effect until the network tasks are stopped and restarted, while other changes do not take effect until you IPL your VS system.

UPDATING STATUS INFORMATION

There are two ways to update a CNS Manager summary or detailed status screen:

- Manually
- Automatically

You can manually update the current status screen by pressing ENTER. The CNS Manager requests the latest statistical information before displaying this information on your screen.

If you want the status to update automatically at a specified interval, enter a value between 001 and 999 seconds, and then press PF11.

Note: *If you enter 000 or if you erase the current value with the DELETE key, pressing PF11 disables automatic updating. If you enter a low value, CNS performance is affected since CNS must service the update requests in addition to handling normal network traffic.*

USING THE EVENT INQUIRY FACILITY

The Event Inquiry Facility allows you to monitor and scroll through the network messages that have been logged by the LOGTSK program on your local system. Logged messages are written to a daily log file (in the format *Lyymmdd*) in the library named @LOG@ on your designated logger volume, as described earlier in this chapter.

To access the Event Inquiry Facility, press PF17 from any CNS Manager screen. Figure 1-2 shows a sample Event Inquiry facility screen.

The screen displays CNS messages that give real-time information on network activity (e.g., reasons for failed attempts to communicate). After leaving the screen, the messages are stored in chronological order in the daily log file. The Event Inquiry facility allows you to scroll through the messages in the daily log file.

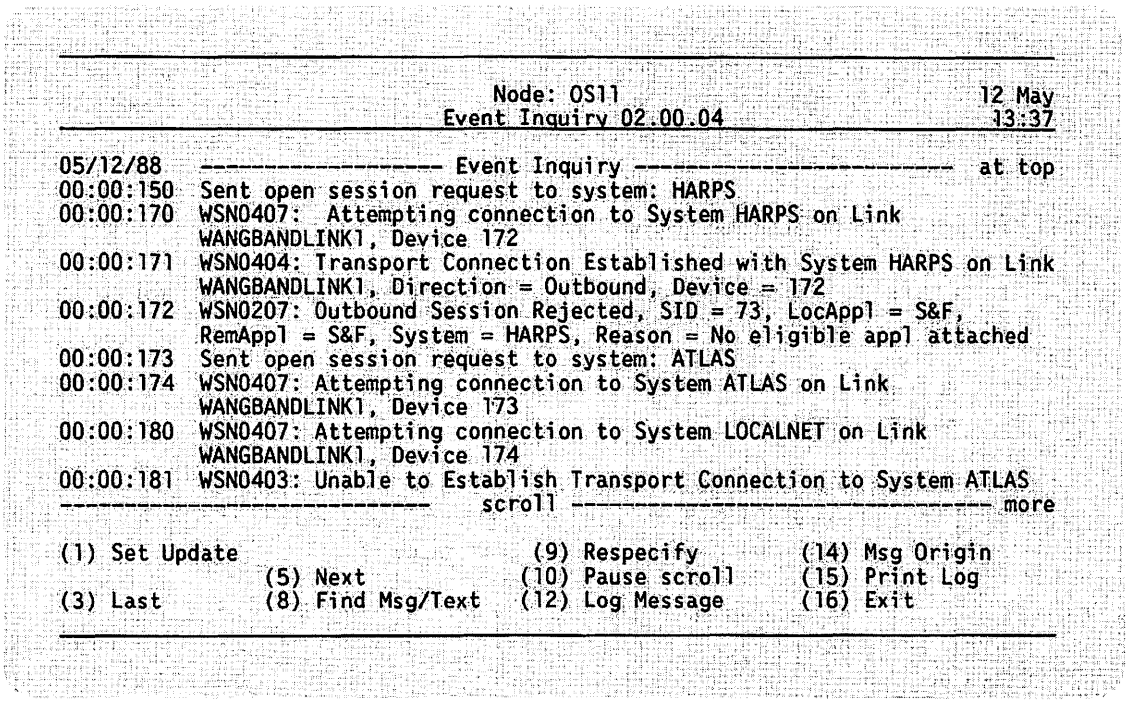

Figure 1-2. Sample Event Inquiry Facility Screen

Functions on the Event Inquiry Screen

When you access the Event Inquiry program, several PF keys appear at the bottom of the screen. These keys and the specific functions are as follows:

PF1 (Set Update) -- Allows you to set the update interval (in seconds) for CNS message updates to the Event Inquiry screen. The CNS Manager retrieves the latest messages from the log file at the specified polling interval. You can specify any value from 0 through 999 seconds. If you specify 0 or leave the input field blank, CNS message updates do not occur.

PF2 (First) -- Displays the first screen of log messages. These messages are the first messages listed in the first log file in Library @LOG@. A new log file is created for each day. Messages in the log file are listed in chronological order, according to the time at which the events they record occurred.

PF3 (Last) -- Displays the latest log messages stored in the log file. If you press PF3, PF10 (Pause Scroll) becomes active. Press PF10 to inhibit automatic scrolling; press PF10 again to restore automatic scrolling.

PF4 (Previous) -- Displays the previous screen of log messages. PF4 also allows you to scroll back to earlier messages in the log. To scroll back, keep pressing PF4.

PF5 (Next) -- Displays the next screen of log messages. To scroll to the end of the log, keep pressing PF5.

PF8 (Find Msg/Text) -- Displays three new fields on the Event Inquiry screen. These fields allow you to search for specific messages in the log file. The fields are

YYMMDD -- Allows you to enter a specific date in YYMMDD format. If you enter information in this field without entering information in the other fields, the screen displays first messages that were logged on the specified date. You can then scroll through the remainder of the messages.

HHMMSS -- Allows you to enter a specific time during the day that was indicated in the YYMMDD field. Enter the time in the HHMMSS format. You should fill in the entire field. The first message that was logged at the specified time (or after) appears on the screen, followed by the chronological listing of any subsequent messages.

Text -- Allows you to search for occurrences of a text string. If you enter text in this field and specify a date and time in the other fields, the YYMMDD and HHMMSS fields are overridden. It does not matter whether you enter text in upper or lower case. However, if the text for which you are searching contains quotation marks, you must enter the quotation marks.

You can also use the Text field to search for messages that contain a specified text string. For example, you might want to enter "Session." Many log messages contain this specific word. The Event Inquiry facility then displays the most recent occurrence of a message with the word "Session." You can press ENTER to scroll back through the log file to earlier messages with the occurrence of the word "Session." You can press PF8 (Find Next) to scroll forward through the log file to find other messages with the word "Session."

Press ENTER after you have typed in the appropriate information in the YYMMDD, HHMMSS, or Text field. This action initiates the search operation. Press PF1 to exit the find function.

PF9 (Respecify) -- Allows you to change the current criteria to display the messages associated with your local system's activity with a specific system and/or subsystem. When you press PF9, a prompt appears on lines 19 and 20, instructing you to enter a system name or "ALL," as well as a subsystem name, subsystem ID, or "ALL." The subsystem name is the 8-character name of the subsystem. A subsystem is a network component that logs messages to the daily log file. The CNS Manager Event Inquiry facility displays messages that are logged by CNS. However, if you want to see messages that are written by other network components, such as Store and Forward and Connection Manager, specify "ALL."

Enter the system name and/or subsystem ID to display only those messages that are associated with that system and/or subsystem. Press PF1 (CANCEL select) to cancel your selection. ALL systems is the default criteria for the display of messages on the Event Inquiry screen. Refer to Appendix A for a complete listing of subsystem IDs.

PF10 (Pause/Resume Scroll) -- Enables you to stop the messages on the log display section of the screen from scrolling automatically. Press PF10 to "freeze" the messages on the screen; press PF10 again to resume automatic scrolling.

PF12 (Log Message) -- Allows you to create and send a message to the daily log file on your local system. Type your message on the message line and press ENTER. Your message appears on the screen at the next update interval. To cancel the log message function, press PF1 (CANCEL log msg).

PF14 (Msg Origin) -- Displays information associated with the origin of a message. Messages are logged by your local system, as well as from remote systems that are communicating with your local system. Position the cursor next to a message on the screen and press PF14. The resulting information (displayed just above the PF key selections on the screen) includes the originating node and subsystem, as well as the date and time the message was logged.

PF15 (Print Log) -- Enables you to print the log messages stored in the daily log file. When you press PF15, the fields that appear at the bottom of the screen allows you to enter the range (between specific dates and times) of log messages you wish to print. For example, you can print all the messages that were displayed from 3 p.m. on 01/10/88 to 10 a.m. on 01/12/88. The fields that appear when PF15 is pressed are

From date/time -- Log messages are stored in the log file according to the date and time they were originally logged. The "From" date/time field allows you to specify the date and time of the message you want to print first. The date field defaults to the current date; the time field defaults to 0 (the beginning of the day). To change the date default setting, enter the new date in YYMMDD format; to change the time default setting, enter the new time in HHMMSS format.

To date/time -- The "To" date and time field allows you to specify the date and time of the message you want to print last. The date field defaults to the current date; the time field defaults to the current time. Change the default settings for the "To" fields as you would change those for the "From" fields.

Note: *If the date and time you specify in the "From" fields is earlier than the date and time you specify in the "To" fields, the messages print out in chronological order. If the date and time in the "To" fields is earlier than the date and time in the "From" fields, the messages print out in reverse chronological order.*

Press ENTER when you have specified the range of specific dates and times, or press PF1 (Cancel print) to cancel the print function. If you press ENTER to print, a message informs you that the print is in progress. When the messages are through printing, a message informs you that the print is completed.

PF16 -- Enables you to exit from the Event Inquiry Facility.

CHAPTER 2
CONTROLLING AND MONITORING TRANSPORTS

OVERVIEW

The CNS Manager allows you to control and monitor the CNS transports defined for the local VS. These transports were defined in the local-view configuration file when WSNEDIT was run to create the local-view configuration (refer to the *VS Network Configuration Guide*).

Transports are responsible for the movement of data between adjacent nodes within a WSN framework. Transports are able to detect data transmission errors, retransmit data, and report problems to other network software components. The CNS Manager allows you to manage these transports from your local VS system.

When an application on the local system attempts to establish a session with an application on a remote system, a transport on the local system establishes a transport connection with the corresponding transport on an adjacent system. The transport connection (hardware and software) remains established until the value set on the transport's inactivity timer (configured in WSNEDIT) is reached; that is, the application is no longer using the transport.

Adjacent systems are directly connected; that is, there are no intermediate systems between them. An application on the local system can establish a session with applications on both adjacent and nonadjacent systems. If the remote system is nonadjacent, the appropriate transports connecting intermediate systems must establish transport connections. Refer to the *VS Network Configuration Guide* for more information on adjacent systems.

The CNS Manager Transports function displays information about the CNS transports defined for the local system. This information includes

- The current status (enabled or disabled) of all transports that have been defined through WSNEDIT

- The number of bytes and messages sent and received since the transport was first enabled
- The number of outgoing messages rejected
- The Base and total cost for the transport
- The Reactivation timer value for the transport

The Transports function also allows you to enable and disable transports and to reconfigure the base cost and reactivation timer values.

ACCESSING THE CNS MANAGER TRANSPORTS FUNCTION

To access the CNS Manager Transports function, press PF5 on the CNS Manager Summary Status screen. The Select CNS Transport for Management screen appears (Figure 2-1).

```
                        Wang Laboratories, Inc.                      12 May
                     Distributed Management Facility                  08:40

                      - CNS Manager Detailed Status -
                     Select CNS Transport for Management

Manager Status:     ACTIVE                 CNS Status:  ACTIVE
Manager Rev:        01.00.00               CNS Rev:     04.01.00
                                           System:      UPTOWN

Place a non-blank character beside the desired transport(s) to select:

    Transport Name      Status          Transport Name      Status
  _ TRANSPORTNAME001    Enabled       _ TRANSPORTNAME006    Enabled
  X TRANSPORTNAME002    Enabled       _ TRANSPORTNAME007    Disabled
  _ TRANSPORTNAME003    Enabled       _ TRANSPORTNAME008    Enabled
  _ TRANSPORTNAME004    Enabled       _ TRANSPORTNAME009    Disabled
  _ TRANSPORTNAME005    Enabled       _ TRANSPORTNAME010    Disabled

           Press (ENTER) to update status or (17) for Event Inquiry
                    (7) Enable    (10) Manage transport(s)    (16) Return
(3) Last  (5) Next  (8) Disable   (11) Update 060 secs        (32) Menu
```

Figure 2-1. Select CNS Transport for Management Screen

The screen lists the names of transports defined for the VS system when WSNEDIT was run to create the local-view configuration. For each transport, the screen lists the transport name and the current transport status. You can manage any number of transports on this screen by placing a nonblank character next to each transport name and then pressing PF10 (Manage transport(s)).

The following fields appear on the Select CNS Transport for Management screen:

Manager Status -- The current state of the CNS Manager background task at the local system. If you do not have the Distributed Management Facility, the status is always ACTIVE.

CNS Status -- The current status of CNS on the local system. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE, you can stop CNS by pressing PF2 from the CNS Manager Summary Status screen.

INACTIVE -- If the CNS status is INACTIVE, you can start CNS by pressing PF1 from the CNS Manager Summary Status screen.

TIMEOUT -- The CNS Manager has sent a message to CNS, but no response has been received.

Manager Rev -- The version of the CNS Manager currently running on the local system.

CNS Rev -- The current version of CNS on the local system.

System -- The name of the local system; that is, the system onto which you are logged.

Transport Name -- The names of the transports that were entered when WSNEDIT was run to create or modify the local-view configuration file for the system.

Status -- The status of the transport acquired from the latest CNS status request. The status messages are as follows:

Enabled -- A transport is enabled when it has successfully performed the functions required to initialize itself for use by CNS. This means that the transport is ready to establish a connection to another system.

Disabled -- A transport is disabled when it is not ready to establish a connection. Either the transport was never enabled, or a user has removed its enabled status.

Pending Enabled -- Pending Enabled appears when a transport is in the process of being enabled.

Pending Disabled -- Pending Disabled appears when a transport is in the process of being disabled.

Enable Failed -- Enable Failed appears when an attempt to enable a transport fails or an enabled transport loses its enabled status without operator intervention.

Disable Failed -- Disable Failed appears when an attempt to disable a transport fails.

Functions on the Select CNS Transport Screen

Table 2-1 describes the function keys that appear on the Select CNS Transport screen.

Table 2-1. Select CNS Transport Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of transports when the list occupies more than one screen.
PF7 (Enable)	Enable one or more transports. Select the transport(s) by typing any nonblank character in the field to the left of the transport name. When you press PF7, the screen displays the message "WARNING: Transport(s) will be enabled, (ENTER) to continue or (16) to return."
PF8 (Disable)	Disable one or more transports. Select the transport(s) by typing any nonblank character in the field to the left of the transport name. When you press PF7, the screen displays the message "WARNING: Transport(s) will be disabled, (ENTER) to continue or (16) to return." **Note:** *If you press PF8 to disable a transport, all sessions currently supported by the transport are terminated, unless there is another transport to the destination system.*
PF10 (Manage Transport(s))	Display the Control/Monitor CNS Transports screen to perform control functions on the selected transport(s).

(continued)

Table 2-1. Select CNS Transport Screen Functions (continued)

When You Press	You Can
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 to 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Manager Summary Status screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS transport status information.

MANAGING THE CNS TRANSPORTS

After you select the transport(s) on the Select CNS Transport for Management screen, press PF10 (Manage Transport(s)) to display the Control/Monitor CNS Transports screen (Figure 2-2).

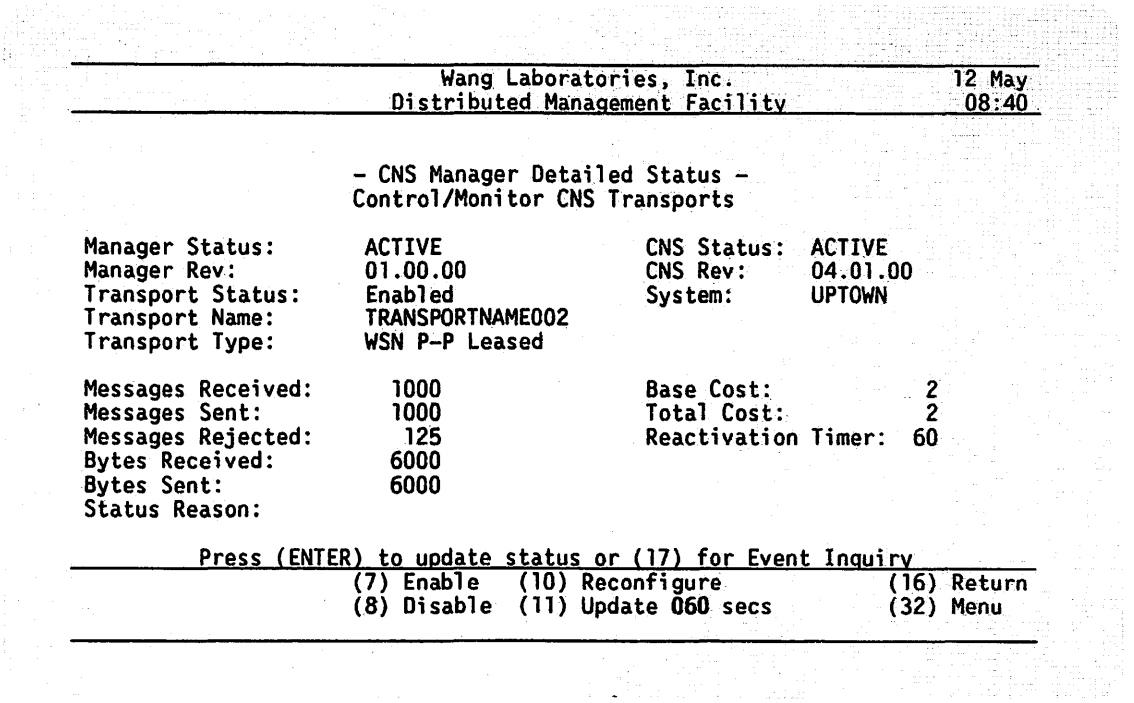

Figure 2-2. Control/Monitor CNS Transports Screen

The screen lists the statistics associated with the first transport that you selected from the Select CNS Transport for Management screen. To display the statistics associated with other selected transports, use the scroll functions (PF2 - PF5).

The following fields appear on the Control/Monitor CNS Transports screen:

Manager Status -- The current state of the CNS Manager background task at the local system. If you do not have the Distributed Management Facility, the status is always ACTIVE.

CNS Status -- The current status of CNS on the local system. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE, you can stop CNS by pressing PF2 from the CNS Manager Summary Status screen.

INACTIVE -- If the CNS status is INACTIVE, you can start CNS by pressing PF1 from the CNS Manager Summary Status screen.

TIMEOUT -- The CNS Manager has sent a message to CNS, but no response has been received.

Manager Rev -- The version of the CNS Manager currently running on the local system.

CNS Rev -- The current version of CNS on the local system.

Transport Status -- The status of the transport acquired from the latest CNS poll. The Status messages are as follows:

Enabled -- A transport is enabled when it has successfully performed the functions required to initialize itself. These functions include establishing transport connections.

Disabled -- A transport is disabled when it is not enabled, either because it was never enabled or because an operator has removed its enabled status.

Pending Enable -- Pending Enable appears when a transport is in the process of being enabled.

Pending Disable -- Pending Disable appears when a transport is in the process of being disabled.

Enable Failed -- Enable Failed appears when an attempt to enable a transport fails or an enabled transport loses its enabled status without operator intervention.

Disable Failed -- Disable Failed appears when an attempt to disable a transport fails.

System -- The name of the local system; that is, the system onto which you are logged.

Transport Name -- The names of the transports that were entered when WSNEDIT was run to create or modify the local-view configuration file for the system.

Transport Type -- The type of transport that was specified when WSNEDIT was run to create or modify the local-view configuration file for the system (e.g., WSN Point-to-Point, WSN Multipoint).

Messages Received -- The number of messages that the system has received via the transport since the transport was last enabled.

Messages Sent -- The number of messages the system has sent via the transport since the transport was last enabled.

Messages Rejected -- The number of outgoing messages that the transport could not deliver since the transport was last enabled.

Note: *A message is the unit of information transfer. Each message consists of a certain amount of control information (e.g., headers) and, in most cases, user data. However, messages may also consist of just control information (e.g., restart commands) used by the network.*

Bytes Received -- The number of bytes that the system has received via the transport since the transport was last enabled.

Bytes Sent -- The number of bytes that the system has sent via the transport since the transport was last enabled.

Status Reason -- A message number that explains the reason for a transport failure. The possible messages are described in Appendix B.

Base Cost -- The Base cost of the transport as specified when the transport was configured in the WSNEDIT utility. (The Base cost is the initial cost of communicating over a transport. The switching layer uses the Base cost to select a transport when there is more than one transport to an adjacent system. The Base cost establishes an initial value used to determine the total cost (including congestion cost) of communicating by means of a transport; see Total Cost.

Base cost is explained in detail in the *VS Network Configuration Guide*.

Total Cost -- The total cost of the transport is equal to the sum of the Base cost and a Congestion Level factor. The Congestion Level factor is a value that a transport sends to CNS whenever CNS loads data to the transport faster than it can be transmitted. CNS then adds this value to the base cost to determine the total cost. If other transports are available to send data, CNS uses the total cost to select the transport with the least congestion.

A transport is not heavily loaded if its base cost is equal to its total cost. For example, a transport whose base and total costs are both equal to 6 is not carrying much traffic. On the other hand, a transport whose base cost is 6 and whose total cost is 9 is experiencing a good deal of congestion. The congestion factor is 3.

Reactivation Timer -- The reactivation timer displays the amount of time (in seconds) that CNS will wait after detecting that a transport cannot deliver data before making another attempt to send the data. The initial value is the value that was set with the WSNEDIT utility. Refer to the *VS Network Configuration Guide*.

Functions on the Control/Monitor Transports Screen

Table 2-2 describes the functions that appear on the Control/Monitor Transports screen.

Table 2-2. Control/Monitor Transports Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through CNS Control/Monitor Transports screens if you selected more than one CNS transport to manage.
PF7 (Enable)	Enable the transport, if this key is displayed. When you press PF7, the screen displays the message "WARNING: Transport(s) will be enabled, (ENTER) to continue or (16) to return."
PF8 (Disable)	Disable the transport, if this key is displayed. When you press PF8, the screen displays the message "WARNING: Transport(s) will be disabled, (ENTER) to continue or (16) to return." ***Note:*** *If you disable a transport, all sessions currently supported by the transport are terminated, unless there is another enabled transport to the destination system.*
PF10 (Reconfigure)	Reconfigure a transport's base cost and reactivation timer at the local system.
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field are 0 - 999. After specifying the value, press PF11. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the Select CNS Transport for Management screen.

(continued)

Table 2-2. **Control/Monitor Transports Screen Functions** (continued)

When You Press	You Can
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS transport status information.

Reconfiguring a CNS Transport

Press PF10 to modify the Base cost and the Reactivation timer. When you press PF10, these fields appear in modify (highlighted) mode. You can then enter new Base cost and Reactivation timer values in these fields. Press ENTER to accept the new values. The screen displays the message "WARNING: Transport will be reconfigured, (ENTER) to continue or (16) to return."

Note: *Modifying the base cost temporarily and dynamically modifies the information that CNS uses to make a routing decision. You should exercise caution before you reconfigure a CNS transport.*

CHAPTER 3
MONITORING APPLICATIONS AND SESSIONS

OVERVIEW

The CNS Manager allows you to monitor all of the sessions in which applications on the local VS are involved. CNS assigns a unique ID to each session at the originating and destination systems. You can determine the amount of session activity involving applications on the local VS and take measures to reduce this activity if you consider it excessive.

The CNS Manager also allows you to monitor all of the applications that are currently attached to CNS. An application is said to be attached when CNS provides the application with full access to the network. An application can be the WSN File Transfer Service (identified as FTM to CNS), Wang OFFICE Store-and-Forward (S&F), Directory Synchronization (DIRSYNC), or others. The Monitor Applications function enables you to determine the amount of network activity in which these applications are involved.

UNDERSTANDING APPLICATIONS AND SESSIONS

A session is a sequenced stream of data between two applications. The application at the local system is called the local application. The application at the remote system is called the remote application. Each application must attach to CNS through an ATTACH command at its respective system before a session can be established.

When the local application attempts to establish a session with a remote application, the End-to-End layer where the local application resides sends a connect request to the remote system. A connect request is a header attached to an OPEN command message that is sent when the application attempts to initiate a session through an OPEN command.

If the connect request is accepted at the remote system, the application at the remote system returns a Connect Accept message to the originating system. The session cannot be established until the Connect Accept header is returned. Once a session is established, two session partners (local and remote) are actively communicating.

If the remote system rejects the connect request, the Application layer at the remote system returns a Connect Reject header.

During a session, the CNS End-to-End layers on the systems at which the respective session partners reside exchange units of network control information called *credits*. For every credit carried on a credit message (or data message), the session partner on the receiving end can send one message. More than one credit can be sent in one credit message. A message is a unit of data transfer that consists of control information (e.g., headers) and, in most cases, user data.

An application attaches to CNS by means of a command called ATTACH that interfaces with the CNS Presentation layer. Once the application is attached to CNS, the CNS Presentation layer can map data from the application into the network during a session. The Presentation layer then insures that the data is delivered to the session partner (i.e., the peer application at the remote system) in the same format in which it was sent.

When an application attaches to CNS, CNS allocates an initial number of credits to the application. The number of credits an application receives from a remote system is added to this initial value.

Suppose that application A and application B are involved in a session. The End-to-End layer on the system where application A resides sends five credit units on one credit message to the End-to-End layer on the system where application B resides. This means that the session partner on application B can send five messages to its remote session partner on application A. The CNS End-to-End layer on the system where application A resides will then send more credit units for that session. Credit units are used for flow control, allowing each application to "pace" its remote session partner.

A session partner can receive only so many messages before it must acknowledge that they have been received. The receiving session acknowledges by sending a unit of network control information called an *acknowledgment* to the session partner that sent the data. Acknowledgments are sent on data messages whenever possible.

Figure 3-1 illustrates the way in which systems exchange credit units, messages with user data, and acknowledgments during a session.

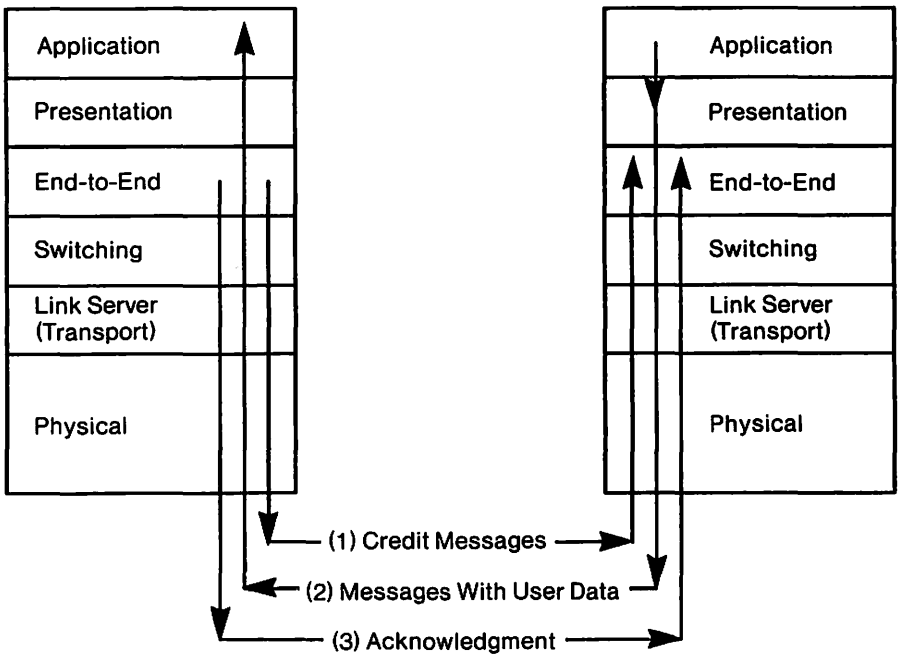

Figure 3-1. Credits, User Messages, and Acknowledgment Exchange

Whenever the End-to-End layer sends data to a remote system, the End-to-End layer starts a "wait-for-acknowledgment" timer. Expiration of the timer before receipt of an acknowledgment causes CNS to attempt to retransmit the messages. The number of retransmission attempts CNS makes corresponds to a preset NAI retry count. If the number of retransmission attempts exceeds the retry count, CNS declares an error condition and terminates the session. Receipt of an acknowledgment prior to the timer expiration indicates successful reception of all messages sent up to that sequence number on the acknowledgment.

CNS saves messages that may have to be retransmitted. CNS releases the message when an acknowledgment is received. This ensures the end-to-end delivery of data.

Each message of transmitted data is assigned a sequence number in the order that it is sent. CNS uses the sequence number to insure that received data is reconstructed in proper order. Suppose that messages labeled 1, 2, 3, and 4 have been sent. If 4 were to arrive at the destination session partner before 3, the CNS End-to-End layer would resequence the data and deliver it to the application in the correct order.

To terminate a session, an application sends a Close request on that session to its session partner. The CNS session does not terminate until the End-to-End layer on the system where the session partner resides acknowledges the Close request.

ACCESSING THE CNS MANAGER APPLICATIONS/SESSIONS FUNCTION

To access the CNS Manager Applications/Sessions function, press PF7 on the CNS Manager Summary Status screen. The Select Application or Session To Monitor screen appears (Figure 3-2).

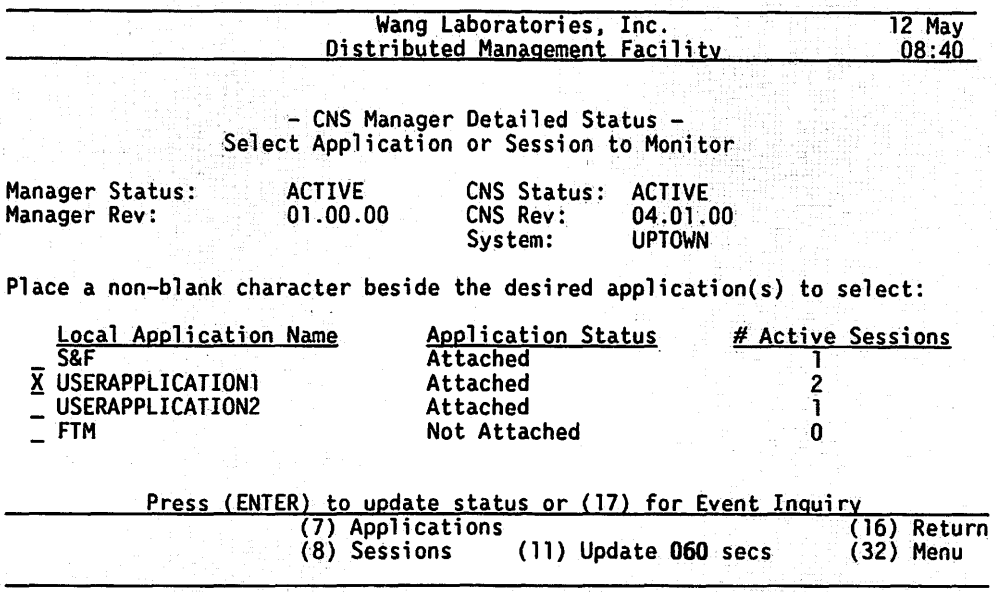

Figure 3-2. Select Application or Session To Monitor Screen

The Select Application or Session To Monitor screen displays the status of each application on the local system (Attached or Not Attached). The screen also displays the number of CNS sessions that are currently active between a local application and a remote application.

Functions on the Select Application or Session To Monitor Screen

Table 3-1 describes the functions on the Select Application or Session To Monitor screen.

Table 3-1. Select Application or Session To Monitor Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of applications when the list consists of more than one screen.
PF7 (Applications)	Monitor the selected application(s).
PF8 (Sessions)	Select an active session to monitor.
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field are 0 - 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Manager Summary Status screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS status information.

MONITORING SESSIONS

To monitor an active session between a local application and a remote application, place a nonblank character next to an application that has an Attached status, with at least one active session, and press PF8. The Select Sessions To Monitor screen appears (Figure 3-3).

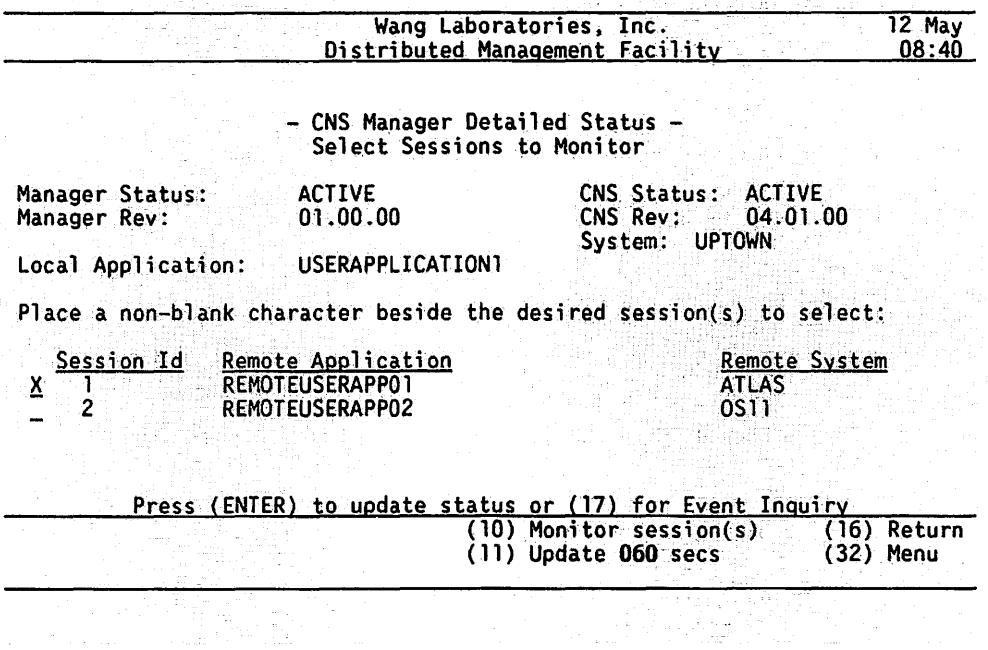

Figure 3-3. Select Sessions To Monitor Screen

The Select Sessions To Monitor screen displays information about each session that is currently active. This information includes

- The application name of the local session partner
- The application name of the remote session partner(s)
- The name of the system at which the remote session partner resides
- The session ID of the session

The following fields appear on the Select Sessions To Monitor screen:

Local Application -- The application name of the local session partner.

Session Id -- The session ID that CNS assigns to each session. The session ID uniquely identifies the session to CNS.

Note: *If NETCORE 8.32 is installed, the term "local" may be displayed next to the session ID. This indicates that two applications on the same system are using CNS as an agent to communicate. CNS performs the Open, Accept, and Close requests, but does not actually transmit data between the two applications. Therefore, the CNS Manager displays such sessions as active, and does not indicate any byte count changes.*

Remote Application -- The name of the remote application involved in the session.

Remote System -- The name of the system on which the remote application resides.

Displaying Session Status

When you select a session to a remote application on the Select Sessions To Monitor screen and then press PF10, the Monitor Session screen appears (Figure 3-4).

```
                         Wang Laboratories, Inc.                 12 May
                      Distributed Management Facility            08:40

                     - CNS Manager Detailed Status -
                            Monitor Session

Manager Status:     ACTIVE           CNS Status:  ACTIVE
Manager Rev:        01.00.00         CNS Rev:     04.01.00
                                     System:      UPTOWN
Local Application:  USERAPPLICATION1
Remote Application: REMOTEUSERAPP01

                                                  Sent       Received
Session Status: Opened               Messages:       5             5
Session Id:     1                    Bytes:       1008           771
Remote System:  ATLAS                Acks:           4             1
Direction:      Outbound             Credits:        1             1
Local Id:       6                    Current Seq #:  6             7
                                     Messages Out of Sequence:     0

         Press (ENTER) to update status or (17) for Event Inquiry
                                                          (16) Return
(3) Last  (5) Next                (11) Update 060 secs    (32) Menu
```

Figure 3-4. Monitor Session Screen

The Monitor Session screen displays detailed status information about the session that you selected. This information includes

- The local and remote application names involved in the session
- An indication of whether the local application or the remote application initiated the session (inbound or outbound session)
- The number of messages, bytes, acknowledgments, and credits the local session partner has sent and received during the session
- The number of messages that have been received out of sequence during the session

If you selected more than one session on the Select Sessions To Monitor screen, use PF2 - PF5 from the Monitor Session screen to display the current status of another session.

Press ENTER when you want to update the Monitor Session screen with the latest status information, or press PF11 to modify the time interval for automatic status updates by CNS.

The following fields appear on the Monitor Session screen:

Local Application -- The name of the local application involved in the session.

Remote Application -- The name of the remote application involved in the session.

Session Status -- The status of the session. There are several status types:

Inactive -- An application on the local system is attempting to establish a session with an application on a remote system. However, End-to-End layer restarts have not been exchanged between the two systems. The session is on hold pending the exchange of restarts.

Open Pending Rcv CA (Open Pending Receive Connection Accept) -- A local application is attempting to establish a session with a remote application, but the session will not be completely established until the remote application has sent a connection-accept response to the Connect request.

Open Pending Snd CA (Open Pending Send Connection Accept) -- A remote application is attempting to establish a session with a local application, but the session will not be completely established until the local application sends an acknowledgment that it has accepted the Connect-Accept request.

Opened -- The session is completely established; data transfer can take place in either direction.

Inact Pnd Rcv Cls Ack (Inactive Pending Receive Close Acknowledgment) -- A local application is attempting to terminate a session. This attempt is made when the local application sends a Close request to its session partner at the remote system. However, the session cannot become inactive until CNS receives an acknowledgment of the Close request from the remote system.

Inact Pnd Snd Cls Ack (Inactive Pending Send Close Acknowledgment) -- A remote application is attempting to terminate a session. This attempt is made when the CNS End-to-End layer at the remote system sends a Close request to the CNS End-to-End layer at the local system. However, the session cannot become inactive until the remote End-to-End layer receives an acknowledgment of the Close request from the End-to-End layer at the local system.

Inact Pending Rcv CA (Inactive Pending Receive Connection Accept) -- The local application has sent a connection request to a remote application. However, before the remote application acknowledged that it had received the connection request, the local application attempted to terminate the session. The session terminates as soon as the local application receives the Connect-Accept request.

Session Id -- The session ID that CNS assigns to each session. The session ID uniquely identifies the session to CNS.

Remote System -- The name of the system on which the remote application resides.

Direction -- An indication of whether the remote or the local application initiated session establishment. The field displays Inbound if a remote application initiated session establishment and Outbound if a local application initiated session establishment.

Local Id -- An application can be a partner in more than one session. The local application session ID is the ID that a local application uses for a particular session. This ID allows CNS and the application to distinguish one session from another.

Messages Sent -- The number of data messages sent since the beginning of the current session.

Messages Received -- The number of data messages received since the beginning of the current session.

Note: *A message is a unit of data transfer that includes data and control information (e.g., headers).*

Bytes Sent -- The total number of bytes sent since the beginning of the current session.

Bytes Received -- The total number of bytes received since the beginning of the current session.

Acks Sent -- The number of acknowledgments sent since the beginning of the current session.

Acks Received -- The number of acknowledgments received since the beginning of the current session.

Credits Sent -- The number of credits that have been made available to the application at the remote system since the session was established. Credits are used by CNS for flow control purposes.

Credits Received -- The number of credits that the remote system has made available to the local application since the beginning of the session.

Current Seq # Sent -- The Current Sequence Number Sent is assigned to each message of transmitted data to ensure that the data is reconstructed in the proper order when it is received. The current sequence number sent is the sequence number of the last message sent by the local application.

Current Seq # Received -- The Current Sequence Number Received is assigned to each message of transmitted data to ensure that the data is reconstructed in the proper order when it is received. The current sequence number received is the sequence number of the last message received by the local application.

Messages Out of Sequence -- The number of messages that have been received out of sequence since the session was established.

MONITORING APPLICATIONS

The CNS Manager Applications function (PF7) displays detailed status information about each application that is attached to CNS. This information includes

- The number of messages that the application has sent and received since it attached to CNS
- The number of bytes the application has sent and received since it attached to CNS
- The number of inbound and outbound sessions that are associated with the local application that you are monitoring
- The total number of inbound and outbound sessions that CNS allows for a given application

To monitor a local application, you must first display the Select Application or Session To Monitor screen (Figure 3-2). Select the application you want to monitor by placing a nonblank character next to the application name; press PF7 (Applications). The Monitor Application screen appears (Figure 3-5).

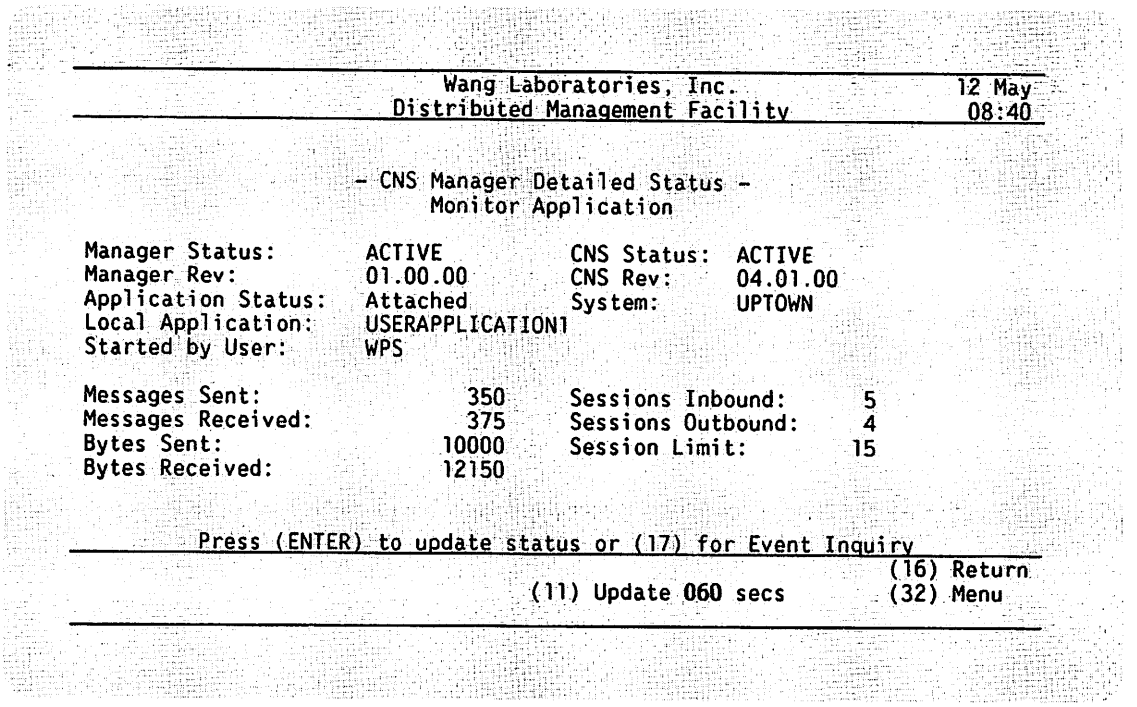

Figure 3-5. Monitor Application Screen

If you selected more than one local application on the Select Sessions To Monitor screen, use PF2 - PF5 on the Monitor Application screen to display the current status of another application.

Press ENTER when you want to update the Monitor Application screen with the latest status information, or press PF11 to modify the time interval for automatic status updates by CNS.

The following fields appear on the Monitor Application screen:

Application Status -- The status of the application on the local system. The status can be Attached or Not Attached to CNS.

Local Application -- The name of the application that you selected from the Select Application or Session To Monitor screen.

Started by User -- Displays the logon ID of the user running the application that is attached to CNS. Applications that attach to CNS are considered network users.

Messages Sent -- The number of messages that the local application has sent since attaching to CNS.

Messages Received -- The number of messages that the local application has received since attaching to CNS.

Bytes Sent -- The number of bytes the application has sent since attaching to CNS.

Bytes Received -- The number of bytes the application has received since attaching to CNS.

Sessions Inbound -- The number of inbound sessions in which the local application is currently involved. Inbound sessions are initiated by remote applications.

Sessions Outbound -- The number of outbound sessions in which the local application is currently involved. Outbound sessions are initiated by the local application.

Session Limit -- The maximum number of inbound sessions allowed by the application as specified by NAI Attach. CNS manages the number of concurrent inbound sessions that it will give to an application; CNS does not manage the number of outbound sessions that it accepts from the application.

CHAPTER 4
MONITORING SYSTEMS AND ROUTES

OVERVIEW

The CNS Manager allows you to monitor routing activity between your local system and a destination system. When you send information to a destination system, CNS uses the routing information that you specified in WSNEDIT, as well as CNS-generated routing records (stored in memory), to establish the least cost path to the destination system/area. A path between your local system and a destination system can consist of a single transport, or it can consist of multiple transports and intermediate systems (or "next hop" systems).

With the CNS Manager Systems/Routes function, you can

- Display the current status of the destination systems that can be reached by your local system
- Select a destination system to display the status of each adjacent system that can link your local system to the destination system
- Select an adjacent system in the path to display the status of the transports (alternate routes) that link your local system with the selected adjacent system

Refer to the *VS Network Configuration Guide* for information on how to configure paths to destination systems and areas (by way of adjacent systems) with WSNEDIT. The guide also explains how CNS generates and uses routing records to send information over the least cost path to other systems/areas in the network.

HOW SYSTEMS COMMUNICATE ACROSS A PATH

A series of protocol level exchanges must take place before two systems can communicate across a given path. The types of protocol level exchanges are as follows:

XID Exchange -- Two adjacent systems exchange XID commands in addition to restart commands. Restart commands determine whether or not two systems (adjacent or non-adjacent) have compatible End-to-End layers. XID commands determine whether or not messages received from an adjacent system's switching layer are accepted (i.e., can pass through or be received) by the receiving system's switching layer. XID commands also determine whether or not a system can send messages to the switching layer of an adjacent system. If an XID command is rejected, communication cannot take place between the adjacent systems. Restarts and XIDs are sent the first time two systems attempt to communicate. They are not exchanged with every session that is opened. Both XIDs and restarts are used for network protocol evolution.

Restart Exchange -- For applications on two systems to communicate across a given path, their respective CNS End-to-End layers must exchange restart commands. A restart command is a unit of network control information that two systems exchange to negotiate the CNS revision level at which they can communicate.

Restart commands are sent by a restart header that identifies the specific system and its CNS revision level. The responding system then sends a unit of network control information called a restart acknowledgment header. The restart acknowledgment notifies the sending system that the revision level carried on its restart request is acceptable.

Two systems running CNS can communicate with each other if they have the same CNS revision level. They can also communicate if one has the CNS revision level that is an immediate successor of the revision level used by the other. The higher CNS revision level makes the final determination as to whether or not communications can take place. CNS communications cannot take place under any other conditions. However, non-CNS systems can communicate with non-CNS adjacent systems.

If a system determines that it cannot communicate with another system, it sends a restart reject header to that system. The restart reject header is a unit of network control information that one system running CNS sends to another when it determines that communication between the two is impossible because CNS revision levels are incompatible.

Figure 4-1 illustrates protocol revision level exchanges.

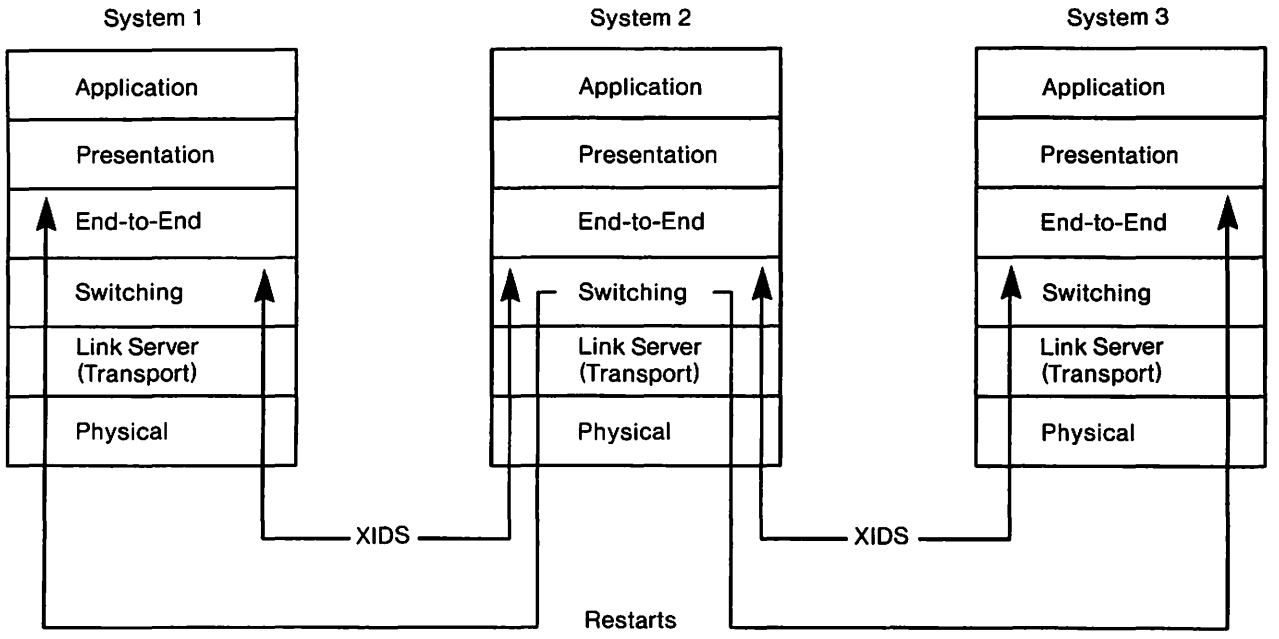

Figure 4-1. Sample Protocol Revision Level Exchanges

In Figure 4-1, system 1 is equipped with CNS revision level N. System 1 can successfully exchange restarts with the system 2, which is also equipped with CNS revision level N. System 1 can successfully exchange restarts with system 3, which is equipped with CNS revision level N-1. The adjacent systems in the illustration can successfully exchange XIDs.

A situation may occur in which an intermediate system on a path between two end point systems is equipped with a CNS revision level that is two steps lower than the revision level installed on one of the end points. Messages can still pass through this intermediate system; however, the intermediate system cannot be a destination for messages originating from the end point with the higher CNS revision level. Figure 4-2 illustrates this situation.

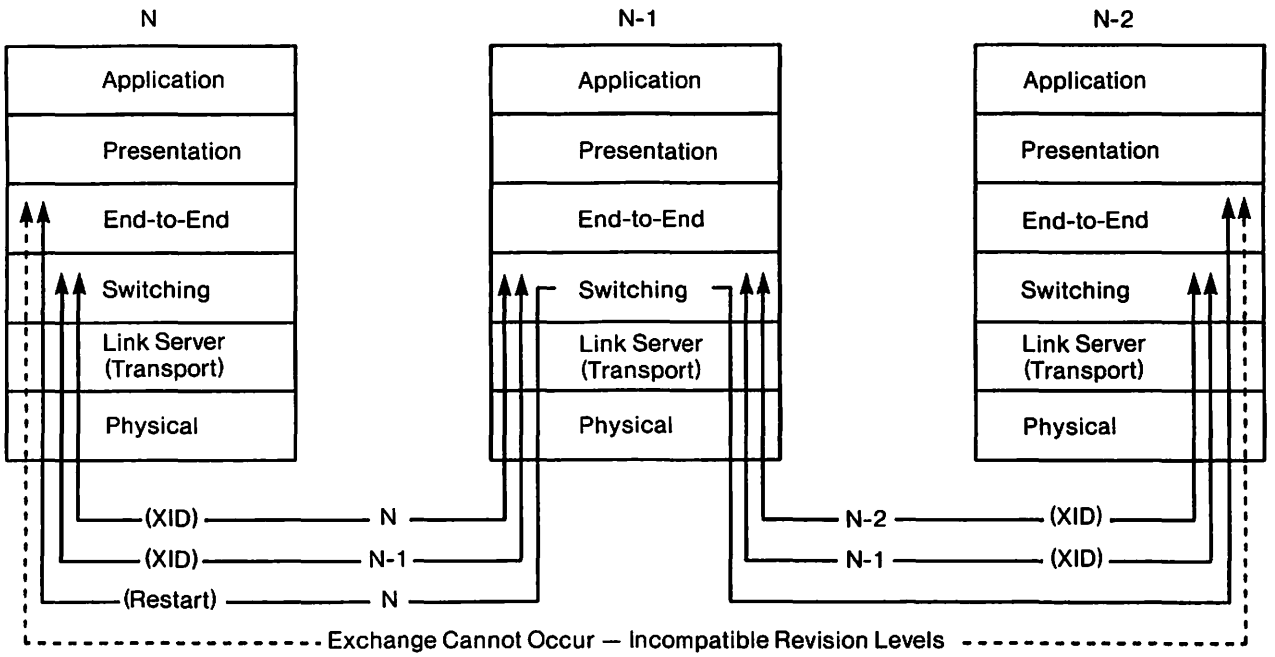

Figure 4-2. Path Through a System With Incompatible CNS Revision Levels

In Figure 4-2, XIDs are successfully exchanged between all the adjacent systems along the path. Due to incompatibility, CNS revision N and CNS revision N-2 cannot exchange restarts. However, messages originating from N that are transmitted to another system can pass through N-2. This pass-through can occur because N-1 has successfully exchanged XIDs with its adjacent systems.

During a session, applications on two adjacent systems use the path with the lowest path cost. If applications on two nonadjacent systems establish a session, multiple transport types can be used to send and receive messages, depending on network congestion and/or the local-view configurations of the endpoint and intermediate systems involved.

Suppose that an application on N in Figure 4-2 attempts to establish a session with an application on another system by way of N-1. Messages can travel from N to N-1 over one transport type (e.g., Wang Band). At N-1, the CNS switching layer can route the message over another transport type (e.g., X.25).

Refer to Chapter 3 for more information on managing sessions.

ACCESSING THE SYSTEMS/ROUTES FUNCTION

Press PF6 from the CNS Manager Summary Status screen to access the Systems/Routes function. The Monitor Systems/Routes screen appears (Figure 4-3).

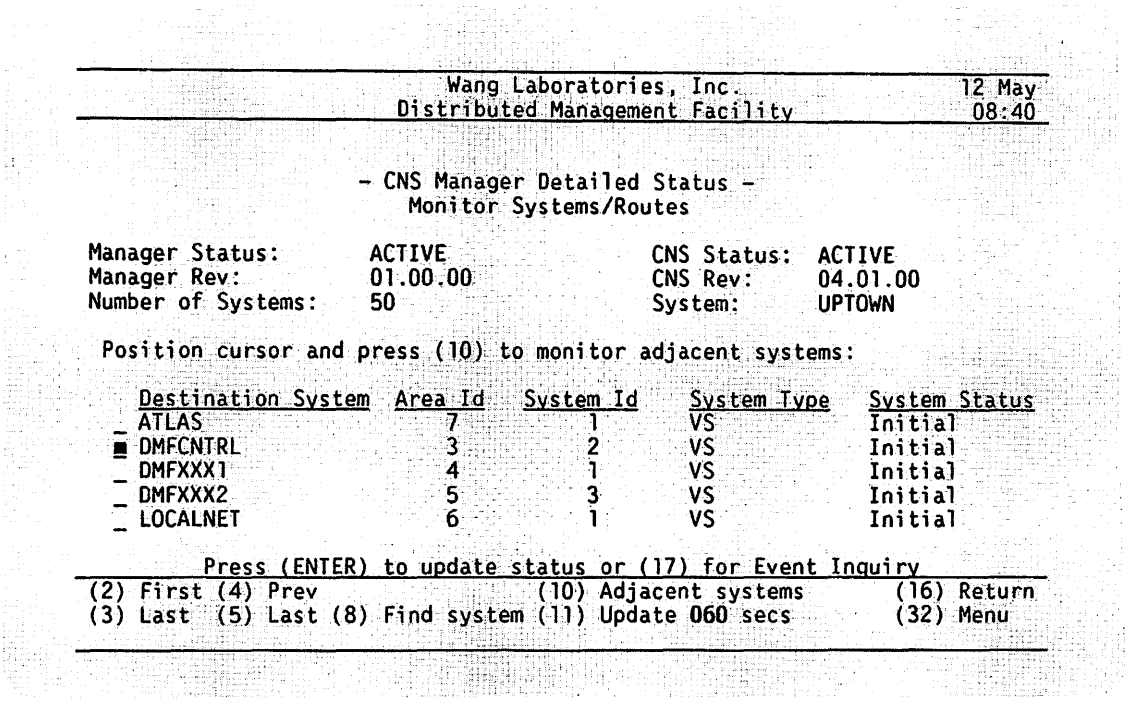

Figure 4-3. Monitor Systems/Routes Screen

The Monitor Systems/Routes screen displays routing activity information. The screen shows the destination systems, area and system IDs, system types, and system status.

The Monitor Systems/Routes screen lists all the destination CNS systems, as defined in the directory file. The fields are as follows:

Manager Status -- The current state of the CNS Manager background task at the local system. If you do not have the Distributed Management Facility, the status is always ACTIVE.

CNS Status -- The current status of CNS on the local system. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE, you can stop CNS by pressing PF2 from the CNS Manager Summary Status screen.

INACTIVE -- If the CNS status is INACTIVE, you can start CNS by pressing PF1 from the CNS Manager Summary Status screen.

TIMEOUT -- The CNS Manager has sent a message to CNS but no response has been received.

Manager Rev -- The version of the CNS Manager currently running on the local system.

CNS Rev -- The current version of CNS on the local system.

Number of Systems -- The number of destination systems that can be contacted by the local system, as configured through WSNEDIT.

System -- The name of the local system; that is, the system onto which you are logged.

Destination System -- The name of the destination system in the local-view directory file defined by WSNEDIT.

Area Id -- The area ID of the destination system, as defined in the directory file by WSNEDIT.

System Id -- The system ID of the destination system, as defined in the directory file by WSNEDIT.

System Type -- The type of CNS system: VS, WPC, PC, or IBM.

System Status -- The status of the system, as follows:

Contacted -- The CNS End-to-End layer on the local VS has successfully exchanged restart commands with the CNS End-to-End layer on the destination system.

Initial -- No attempt has been made to contact the system.

Lost -- An attempt to establish communications with the destination system has failed.

Pending -- An attempt is being made to establish communications with the remote system.

Functions on the Monitor Systems/Routes Screen

Table 4-1 describes the functions that appear on the CNS Manager Monitor System/Routes screen.

Table 4-1. CNS Manager Monitor Systems/Routes Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of systems when the list consists of more than one screen.
PF8 (Find System)	Display the screen containing the system that you specify. Enter the name of the system (or just the first letter of the system name) at the System Name prompt at the base of the screen and press ENTER to accept the selection, or press PF16 to return to the Monitor Systems/Routes screen. ***Note:*** *No leading or embedded blank spaces are allowed in this field. If the system name that is entered contains any blanks, the screen will display the message "Remove leading or embedded blanks."*
PF10 (Adjacent systems)	Monitor the systems that are adjacent to the system that you selected.
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 to 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Manager Summary Status screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.

(continued)

Table 4-1. CNS Manager Monitor Systems/Routes Screen Functions (continued)

When You Press	You Can
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS status information.

MONITORING ADJACENT SYSTEMS

When you position the screen cursor next to a destination system on the Monitor Systems/Routes screen, press PF10 (Adjacent Systems) to display the Monitor Adjacent Systems screen (Figure 4-4). The screen displays the list of systems that are adjacent to the destination system and the way by which messages can be routed to the destination systems.

Figure 4-4 illustrates the Monitor Adjacent Systems screen.

```
                           Wang Laboratories, Inc.                  12 May
                        Distributed Management Facility             08:40

                      - CNS Manager Detailed Status -
                         Monitor Adjacent Systems

Manager Status:        ACTIVE                 CNS Status:  ACTIVE
Manager Rev:           01.00.00               CNS Rev:     04.01.00
Destination System:    DMFCNTRL               System:      UPTOWN
Maximum Adjacent Systems: 3                   Current Adjacent Systems: 3

Position cursor and press (10) to monitor alternate routes:

     Adjacent          Area     System    System  Path      Path   Path
     System            Id        Id       Type    Status    Cost   Reject
   _ ATLAS               7         1        VS    Active       1        0
   ■ DMFXXX1             4         1        VS    Active       1        0
   _ DMFXXX2             5         3        VS    Active       1        0

          Press (ENTER) to update status or (17) for Event Inquiry
                    (7) Modify Cost    (10) Alternate routes    (16) Return
                    (8) Find system    (11) Update 060 secs     (32) Menu
```

Figure 4-4. Monitor Adjacent Systems Screen

The Monitor Adjacent Systems screen displays several fields of information for each adjacent system. These fields are as follows:

Destination System -- The name of the destination system that you selected from the Monitor Systems/Routes screen.

Maximum Adjacent Systems -- The maximum number of adjacent systems that are currently supported by CNS. This is the number of adjacent systems by which CNS can route to a particular destination system.

Current Adjacent Systems -- The current number of adjacent systems by which messages can be routed to the destination system.

Adjacent System -- The list of adjacent systems by which messages can be routed to the destination system.

Area Id -- The area ID of the adjacent system, as defined in the directory file by WSNEDIT.

System Id -- The system ID of the adjacent system, as defined in the directory file by WSNEDIT.

System Type -- The type of CNS system: VS, WPC, PC, etc.

Path Status -- The status of the communications path between the local VS and the adjacent system. There are three possible status types:

Active -- Indicates that the CNS Switching layer on the local VS has successfully exchanged XID commands with the CNS switching layer on the adjacent system.

Inactive -- Indicates that the CNS Switching layer on the local VS and the Switching layer on the adjacent system have not exchanged XID commands. Communications cannot take place across the path until XID commands are successfully exchanged.

Pending -- Indicates that the CNS Switching layer on the local VS has sent an XID command to the Switching layer on the adjacent system. The Switching layer on the local VS is waiting to receive an XID acknowledgment from the adjacent system.

Path Cost -- Displays the Path cost of the route between the local VS and the destination system by way of the adjacent system. The path cost was entered when WSNEDIT was run to configure routes (refer to the *VS Network Configuration Guide*). The least cost path is the primary path. If two paths have the same Path cost, the path listed first is the chosen path.

Path Reject -- Displays the number of messages that could not be delivered to the destination system by way of the adjacent system. Whenever a path reject occurs during a session, the session is automatically terminated, unless an alternate path to that destination exists.

Functions on the Monitor Adjacent Systems Screen

Table 4-2 describes the functions that appear on the CNS Manager Monitor Adjacent Systems screen.

Table 4-2. CNS Manager Monitor Adjacent Systems Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of systems when the list consists of more than one screen.
PF7 (Modify Cost)	Allows you modify the path cost to a specific destination. The screen name changes to Modify Path Cost.
PF8 (Find system)	Display the screen containing the system that you specify. Enter the name of the system at the System Name prompt at the base of the screen and press ENTER to accept the selection, or press PF16 to return to the Monitor Systems/Routes screen. ***Note:*** *No leading or embedded blank spaces are allowed in this field. If the system name that is entered contains any blanks, the screen will display the message "Remove leading or embedded blanks."*
PF10 (Alternate routes)	Monitor the transports that link the local system to the selected adjacent system.

(continued)

Table 4-2. CNS Manager Monitor Adjacent Systems Screen Functions (continued)

When You Press	You Can
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 to 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Manager Monitor Systems/Routes screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS status information.

MONITORING ALTERNATE ROUTES

When you position the screen cursor next to the name of an adjacent system on the Monitor Adjacent Systems screen, you can press PF10 (Alternate routes) to display the list of transports that link your local system to the selected adjacent system.

The local VS uses these transports to communicate with a destination system by way of the adjacent system. The transports were defined when WSNEDIT was run to create the communications configuration for the local VS (refer to the *VS Network Configuration Guide*).

Figure 4-5 illustrates the Monitor Alternate Routes screen.

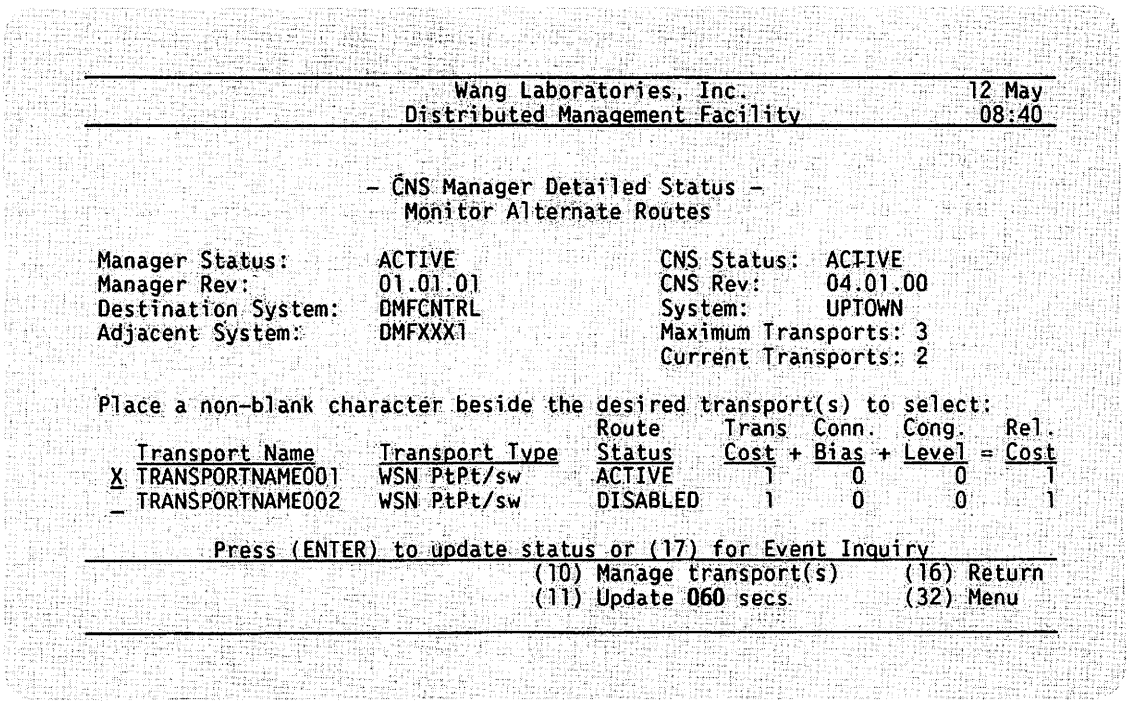

Figure 4-5. Monitor Alternate Routes Screen

The local VS uses the transports listed on this screen to send messages to and receive messages from the adjacent system. The top of the menu displays the maximum and current number of transports that can connect the local VS and the adjacent system. The top of the menu also displays the name of the destination system to which messages will be routed by way of the adjacent system.

The fields that display transport information are as follows:

Destination System -- The system name that you selected on the Monitor Systems/Routes screen.

Adjacent System -- The system name that you selected on the Monitor Adjacent Systems screen.

Maximum Transport(s) -- The maximum number of configured transports that can link your local system to a particular adjacent system.

Current Transports -- The current number of transports that can link the local system to the adjacent system.

Transport Name -- The name of the transport(s) contained in the directory file, as defined by WSNEDIT, that route to the adjacent system.

Transport Type -- The type of transport that was specified when WSNEDIT was run to create or modify the directory file for the system (e.g., WSN Point-to-Point, WSN Multipoint).

Route Status -- The status of the route. The four status types are as follows:

ACTIVE -- A transport connection, or session, is currently established to the adjacent system across the transport.

INACTIVE -- The transport is enabled (i.e., capable of establishing a transport connection) but is not currently supporting a transport connection to the adjacent system.

DISABLED -- The transport is not capable of supporting a transport connection. To enable a transport, you must access the Control/Monitor CNS Transports screen by pressing PF10 (Manage transport(s)) from the Select CNS Transport for Management screen. Refer to Chapter 2 for information on modifying transports at the local system.

BLOCKED -- On a route with multiple enabled transports, the transport is not capable of supporting a connection due to transmission failures. The connection continues on remaining unblocked transports.

Note: *802.3 LAN transports always appear as ACTIVE when they are enabled because they operate in connectionless mode.*

Trans Cost (Transport Cost) -- The Base cost of the transport, as defined in WSNEDIT.

Conn. Bias (Connection Bias) -- A value that enables CNS to favor the use of a transport that has already established a connection. If a transport has not established a connection to an adjacent system, CNS adds a value (ranging from 0 to 2) to that transport's relative cost. The value for connection bias is entered in WSNEDIT. If the route status displays ACTIVE, the connection bias is set to 0.

If two transports are configured between two adjacent systems, connection bias allows CNS to favor the use of the transport that has already established a connection. Connection bias increases the relative cost of the transport that is not connected, causing CNS to minimize the number of transport connections it makes. Thus, connection bias promotes efficiency by limiting use of a backup transport to times when the primary transport is significantly congested. Connection bias applies only to enabled transports.

Cong. Level (Congestion Level) -- A value (1 - 4) that determines the number of messages that can accumulate in the transport queue for a specific adjacent system before a factor is added to the Base cost. There are four congestion levels: Level 1, Level 2, Level 3, and Level 4. Each level is associated with a maximum number of messages. Once the level is reached or exceeded, a congestion level factor of 1 is added to the Base cost. Congestion levels are configured in WSNEDIT.

Rel Cost (Relative Cost) -- Relative cost is a value that is dynamically updated, based on congestion and connection state. Relative cost is determined by the following formula:

Relative Cost = Transport Cost + Congestion Level + Connection Bias

Base cost is a constant that is entered through WSNEDIT (refer to the *VS Network Configuration Guide*). The base cost is factored into the relative cost formula as a *transport cost*. It is the initial factor for prioritizing the selection of one transport over another in an alternate transport or load balancing configuration.

For a more thorough examination of the Relative Cost calculation, refer to the *VS Network Configuration Guide*.

Functions on the Monitor Alternate Routes Screen

Table 4-3 describes the functions that appear on the CNS Manager Monitor Alternate Routes screen.

Table 4-3. CNS Manager Monitor Alternate Routes Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of transports when the list consists of more than one screen.
PF10 (Manage transport(s))	Display the Control/Monitor CNS Transports screen.

(continued)

Table 4-3. CNS Manager Monitor Alternate Routes Screen Functions (continued)

When You Press	You Can
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 to 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Manager Monitor Adjacent Systems screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS status information.

MANAGING TRANSPORTS

When you select a transport on the Monitor Alternate Routes screen, you can press PF10 (Manage transport(s)) to display the Control/Monitor CNS Transports screen. This screen displays the statistics acquired from the latest CNS poll. Refer to Chapter 2 for detailed information on controlling and monitoring CNS transports.

CHAPTER 5
CNS DIAGNOSTICS

OVERVIEW

This chapter describes the diagnostic programs that you can access with the CNS Manager. The CNS Manager Diagnostics function provides a set of programs that can be run on your local system to test CNS activity on your network. The diagnostic test program parameters can be modified to suit the needs of your network.

When you select one of these diagnostic programs and then specify the appropriate parameters, the program attaches to CNS and initiates a session with a peer application at a specified destination system.

Throughput Test (THRUTEST) -- Measures the effective user data in bits per second between two systems.

Propagation Delay Test (PROPTEST) -- Measures the propagation delay for data transfer between systems. The propagation delay is the amount of time it takes to transmit a message to a remote system and back to the originating system. When this program is run, the local system sends one message to a remote system, where the message passes through CNS to PASSTEST. It then goes back through CNS to the originating system.

Synchronous Send/Receive Test (SYNCTEST) -- Verifies the accuracy of data transferred between two systems. When SYNCTEST is run, messages are sent to PASSTEST at the remote system, which returns each message it receives to the originating system. A comparison is then made at the originating system between the messages originally sent and the messages returned. The originating system can detect inconsistencies between the two sets of messages, thereby determining message integrity.

Connect Test (CONECTST) -- Determines which remote systems in the network are running CNS.

The CNS Throughput Test, Propagation Delay Test, and Synchronous Send/Receive Test programs attach to CNS and initiate a session with the application PASSTEST, at a specified destination system. When PASSTEST is attached to CNS, it is identified as DIAG1, a local application, and is included in the list of local applications on the Select Application or Session to Monitor screen. The remote systems involved in these tests start PASSTEST automatically when CNS diagnostic programs are run.

Path Trace -- Allows you to trace the path that a data message will take from the local system to a destination system.

CNS Trace -- Allows you to set trace points within CNS.

ACCESSING THE DIAGNOSTICS FUNCTION

To access the Diagnostics function, press PF10 (Diagnostics) on the CNS Manager Summary Status screen. The CNS Manager Diagnostics screen appears (Figure 5-1).

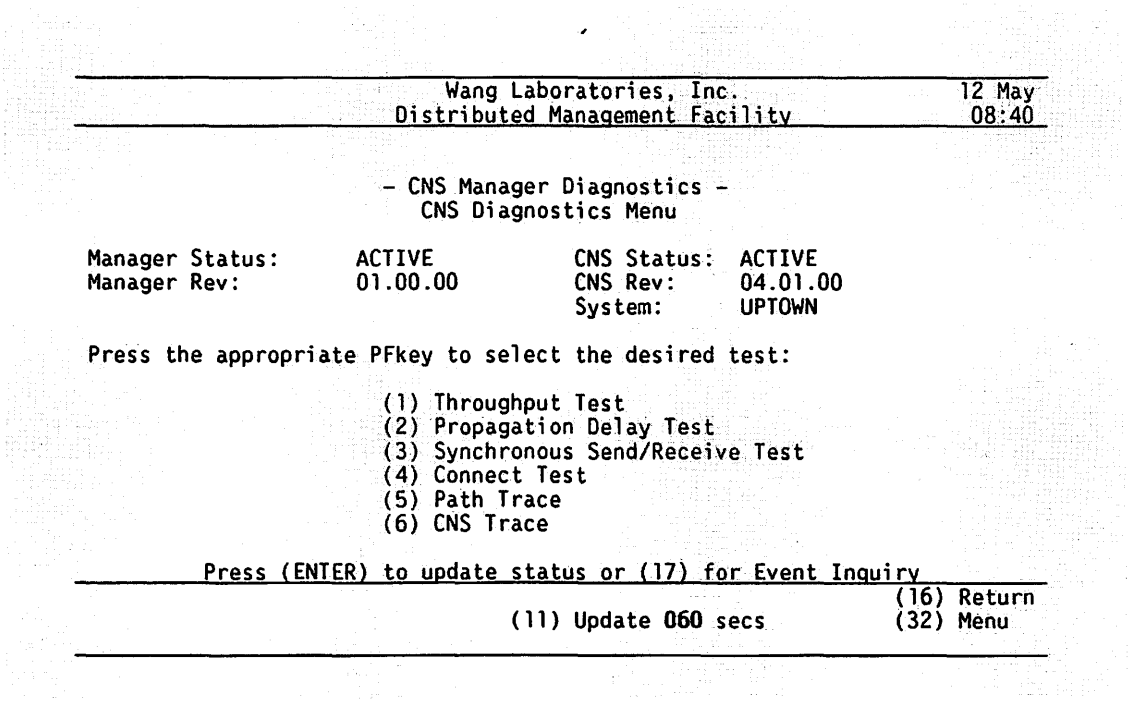

Figure 5-1. CNS Manager Diagnostics Screen

The Diagnostics screen lists six diagnostic programs. To run a diagnostic program, press the appropriate PF key. After selecting a diagnostic program, you must enter the appropriate parameters for that program. This chapter describes each program and the appropriate parameters.

The following fields are displayed on the CNS Diagnostics screen:

Manager Status -- The current state of the CNS Manager background task at the local system. If you do not have the Distributed Management Facility, the status is always ACTIVE.

CNS Status -- The current status of CNS on the local system. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE you can stop CNS by pressing PF2 from the CNS Manager Summary Status screen.

INACTIVE -- If the CNS status is INACTIVE you can start CNS by pressing PF1 from the CNS Manager Summary Status screen.

TIMEOUT -- The CNS Manager has sent a message to CNS, but no response has been received.

Manager Rev -- The version of the CNS Manager currently running on the local system.

CNS Rev -- The current version of CNS on the local system.

System -- The name of the local system; that is, the system onto which you are logged.

Table 5-1 lists the available functions on the CNS Manager Diagnostics screen.

Table 5-1. CNS Manager Diagnostics Screen Functions

When You Press	You Can
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 to 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.

(continued)

Table 5-1. CNS Manager Diagnostics Screen Functions (continued)

When You Press	You Can
PF16 (Return)	Return to the CNS Manager Summary Status screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update CNS status.

USING THROUGHPUT TEST

When you press PF1 on the CNS Manager Diagnostic screen, the THRUTEST Parameters screen appears (Figure 5-2).

The Throughput Test (THRUTEST) Parameters screen allows you to enter the parameters that the program requires to measure the data transfer rate between the local system and a remote system. You must enter these parameters before THRUTEST can make test runs. To delete characters from these fields, position the cursor under the character you want to delete and press DELETE.

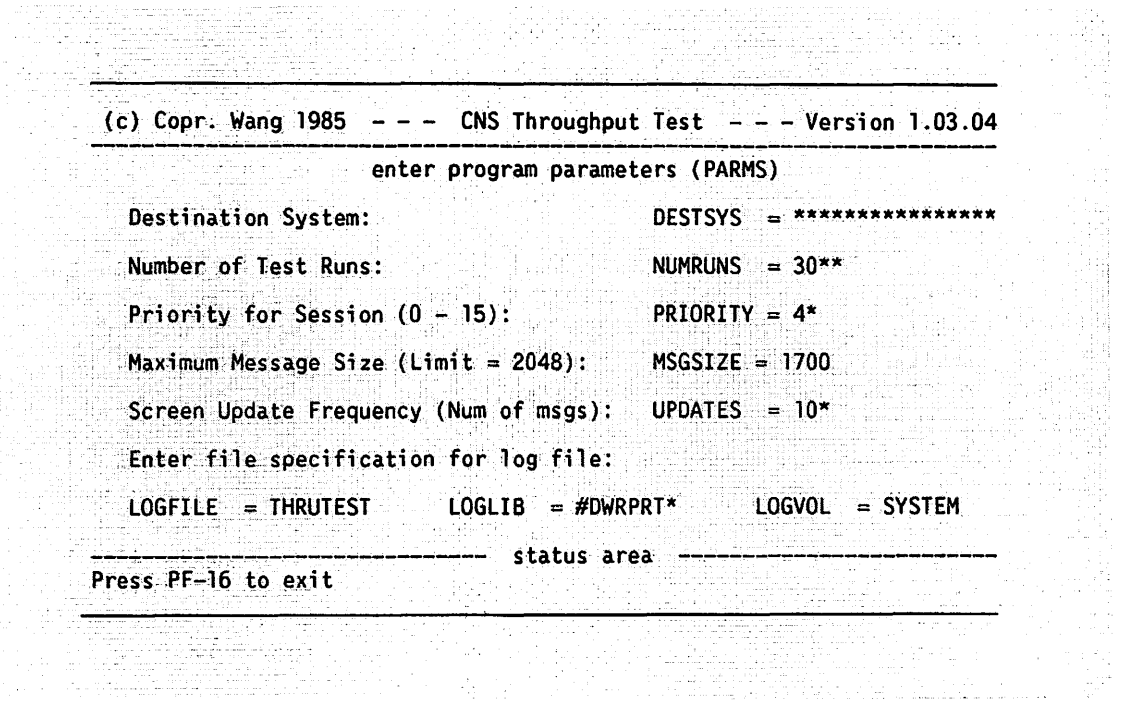

Figure 5-2. THRUTEST Parameters Screen

Specifying the THRUTEST Parameters

To specify the CNS Throughput Test parameters, position the cursor on the parameter to be specified, and enter the desired information. The following fields appear on the THRUTEST Parameters screen:

Destination System (DESTSYS) -- Enter the name of the remote system. The name must be one that was defined in the network directory when WSNEDIT was run to define areas and systems in the network (refer to the *VS Network Configuration Guide*).

Note: *If the destination system name is left blank, DESTSYS defaults to the local system.*

Number of Test Runs (NUMRUNS) -- Enter the number of test runs you want THRUTEST to make. This number specifies the number of times THRUTEST will measure the rate of data transfer between two systems. The accuracy of the test results tends to increase as the number of test runs increases. To obtain meaningful results, you should specify at least 30 runs. The valid values for this field range from 1 to 9999. The default value is 30.

Priority for Session (PRIORITY) -- CNS uses priority windows to manage sessions. Sessions with low priority window values are given greater access to the network than sessions with high priority window values. The THRUTEST test runs tend to be faster if they are assigned low priority window values. The valid values for this field range from 0 to 15. The default value is 4.

Maximum Message Size (MSGSIZE) -- Enter the message size (in bytes) to be allocated to the THRUTEST session. The message size field indicates the maximum size of the message transmitted to the remote system (via THRUTEST). The valid values for this field range from 1 to 2048 bytes (2K). The default value is 1700.

Screen Update Frequency (UPDATES) -- Indicates how many messages will be sent (via THRUTEST) before the THRUTEST parameters screen status area is updated. For example, if you enter 1 in this field, THRUTEST will display the number of every message as it is sent (1, 2, 3, etc.). If you enter the default value 10, THRUTEST will display the number of every tenth message as it is sent (10, 20, 30, etc.). The valid values for this field range from 1 to 999. The default value is 10.

Note: *Because it takes time for THRUTEST to update the status area of the screen, frequent screen updating detracts from achievable throughput. To obtain maximum throughput, set the screen update frequency value high.*

LOGFILE -- Enter the name of the VS print file in which THRUTEST results will be stored. You can use the default name THRUTEST or specify another file.

LOGLIB -- Enter the name of the library in which you want the log file to reside. You can use the default library (your VS print file library) or specify another valid library.

LOGVOL -- Enter the name of the volume on which your log library resides. The default volume is the system volume.

Running THRUTEST

Press ENTER when you have specified the parameters required to run THRUTEST. A series of messages appears on the screen after you press ENTER. These messages provide the following information:

- THRUTEST is attaching to the network.
- An attempt is being made to open a session with the PASSTEST program at the remote system.

- The open attempt has succeeded or failed. If the open attempt fails, an error message is displayed explaining the reason for the failure. You then must press ENTER to continue. The THRUTEST Statistics screen appears, allowing you to exit from THRUTEST or run the program again.

- Test runs are in progress.

- Test runs have been completed and an attempt is being made to close the session with the THRUTEST program at the remote system. An attempt is also being made to detach from the network.

THRUTEST Statistics

When THRUTEST completes the test runs, the THRUTEST Final Statistics screen appears, displaying the statistics gathered during testing. The Final Statistics screen also appears if the THRUTEST program at the remote system could not be contacted and ENTER is pressed to continue. Figure 5-3 shows a sample THRUTEST Final Statistics screen.

```
(c) Copr. Wang 1985  - - - CNS Throughput Test - - -  Version 1.03.01

                        final statistics (stats)

  Number of test runs completed:                          100

  Message size sent:                                      1700

  Priority of session:                                    4

  Total send time for tests run (in 1/100 secs):          139

  Percentage of time waiting for credit:                  0%

  Throughput in Bits Per Second:                          9700

  Hit PF-1 to restart or ENTER/PF-16 to end.
```

Figure 5-3. THRUTEST Final Statistics Screen

The statistics that THRUTEST gathers during testing are as follows:

Number of test runs completed -- Displays the number of test runs made during testing. If this number does not match the number of test runs specified on the THRUTEST Parameters screen, an error has occurred during testing.

Message size sent -- Displays the value entered in the Maximum Message Size field on the THRUTEST Parameters screen. If the two values do not match, an error has occurred.

Priority of session -- Displays the value entered in the Priority for Session field on the THRUTEST Parameters screen. If it does not match, an error has occurred.

Total send time for tests run (in 1/100 secs) -- Displays the time it took to send the messages during the test runs.

Percentage of time waiting for credit -- Displays the percentage of send time in which messages could not be sent due to flow control restrictions.

Throughput in Bits Per Second -- Displays the effective data transfer rate between the THRUTEST on the local system and PASSTEST on the remote system. The effective data transfer rate will, in most cases, be less than the maximum line speed supported. The maximum line speed supported reflects the modem-to-modem data transfer rate. The value that appears in this field is the application-to-application data transfer rate.

When you have finished viewing the information on the THRUTEST Statistics screen, you can press PF1 (Restart) to run THRUTEST again or PF16 (End) to return to the CNS Manager Diagnostics screen. If PF1 is selected, the results of the next execution are appended to the existing log file. If PF16 is selected, the existing log file is deleted the next time the test is run.

USING PROPAGATION DELAY TEST

When you press PF2 on the CNS Manager Diagnostics screen, the Propagation Delay Test Parameters (PROPTEST) screen appears (Figure 5-4).

The Propagation Delay Test (PROPTEST) measures the propagation delay for data transfer between systems. The propagation delay is the amount of time it takes to transmit a message to a remote system and back to the originating system. When this program is run, the local system sends one message to a remote system, where the message passes through CNS to PASSTEST. It then goes back through CNS to the originating system.

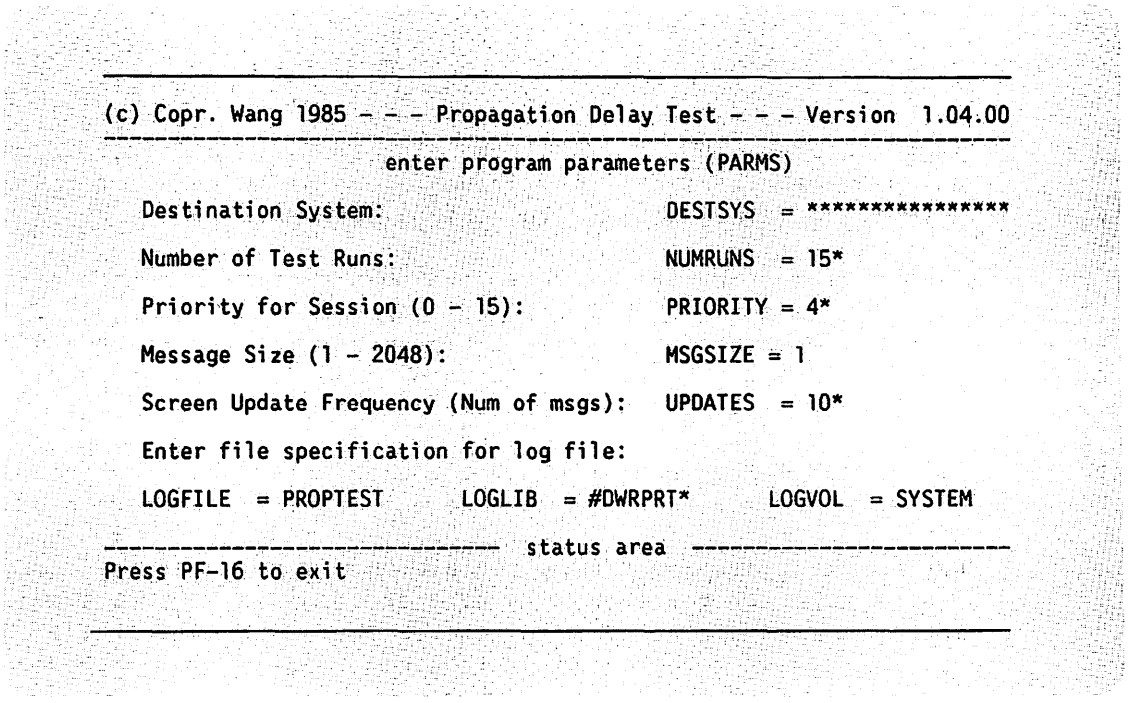

Figure 5-4. PROPTEST Parameters Screen

Specifying the PROPTEST Parameters

You must specify PROPTEST parameters before PROPTEST can make test runs. To specify the parameters, position the cursor on the parameter to be specified, and enter the desired information. To delete characters from these fields, position the cursor on the character you want to delete and press DELETE.

The following fields appear on the PROPTEST Parameters screen:

Destination System (DESTSYS) -- Enter the name of the remote system. The name must be one that was defined in the network directory when WSNEDIT was run to define areas and systems in the network (refer to the *VS Network Configuration Guide*).

Note: *If the destination system name is left blank, DESTSYS defaults to the local system.*

Number of Test Runs (NUMRUNS) -- Enter the number of test runs you want PROPTEST to make. This number specifies the number of times PROPTEST will measure the rate of data transfer between two systems. The accuracy of the test results tends to increase as the number of test runs increases. The valid values for this field range from 1 to 999. The default value is 15.

Priority for Session (PRIORITY) -- CNS uses priority windows to manage sessions. Sessions with low priority window values are given greater access to the network than sessions with high priority window values. The PROPTEST test runs tend to be faster if they are assigned low priority window values. The valid values for this field range from 0 to 15. The default value is 4.

Message Size (MSGSIZE) -- Enter the message size (in bytes) to be allocated to the PROPTEST session. The message size field indicates the maximum size of the message transmitted to the remote system (via PROPTEST). The valid values for this field range from 1 to 2048 bytes (2K). The default value is 1.

Screen Update Frequency (UPDATES) -- Indicates how many messages will be sent (via PROPTEST) before the PROPTEST parameters screen status area is updated. For example, if you enter 1 in this field, PROPTEST will display the number of every message as it is sent (1, 2, 3, etc.). If you enter the default value 10, PROPTEST will display the number of every tenth message as it is sent (10, 20, 30, etc.). The valid values for this field range from 1 to 999. The default value is 10.

Note: *Because it takes time for PROPTEST to update the status area of the screen, frequent screen updating detracts from achievable throughput. To obtain maximum throughput, set the screen update frequency value high.*

LOGFILE -- Enter the name of the VS print file in which PROPTEST results will be stored. You can use the default name PROPTEST or specify another file.

LOGLIB -- Enter the name of the library in which you want the log file to reside. You can use the default library (your VS print file library) or specify another valid library.

LOGVOL -- Enter the name of the volume on which your log library resides. The default volume is the system volume.

Running PROPTEST

After you have specified the PROPTEST parameters, press ENTER. A series of messages appears on the screen after you press ENTER. These messages provide the following information:

- PROPTEST is attaching to the network.
- An attempt is being made to open a session with the PASSTEST program at the remote system.

- The open attempt has succeeded or failed. If the open attempt fails, an error message is displayed that tells you the reason for the failure. You then must press ENTER to continue. The PROPTEST Statistics screen appears, allowing you to exit from PROPTEST or press PF1 to run the program again.

- Test runs are in progress.

- Test runs have been completed and an attempt is being made to close the session with the PROPTEST program at the remote system. An attempt is also being made to detach from the network.

PROPTEST Statistics

When PROPTEST completes the designated number of test runs, the PROPTEST Final Statistics screen appears, displaying the statistics gathered during testing. The same screen also appears if the PROPTEST program at the remote system could not be contacted and ENTER is pressed to continue. Figure 5-5 shows a sample PROPTEST Final Statistics screen.

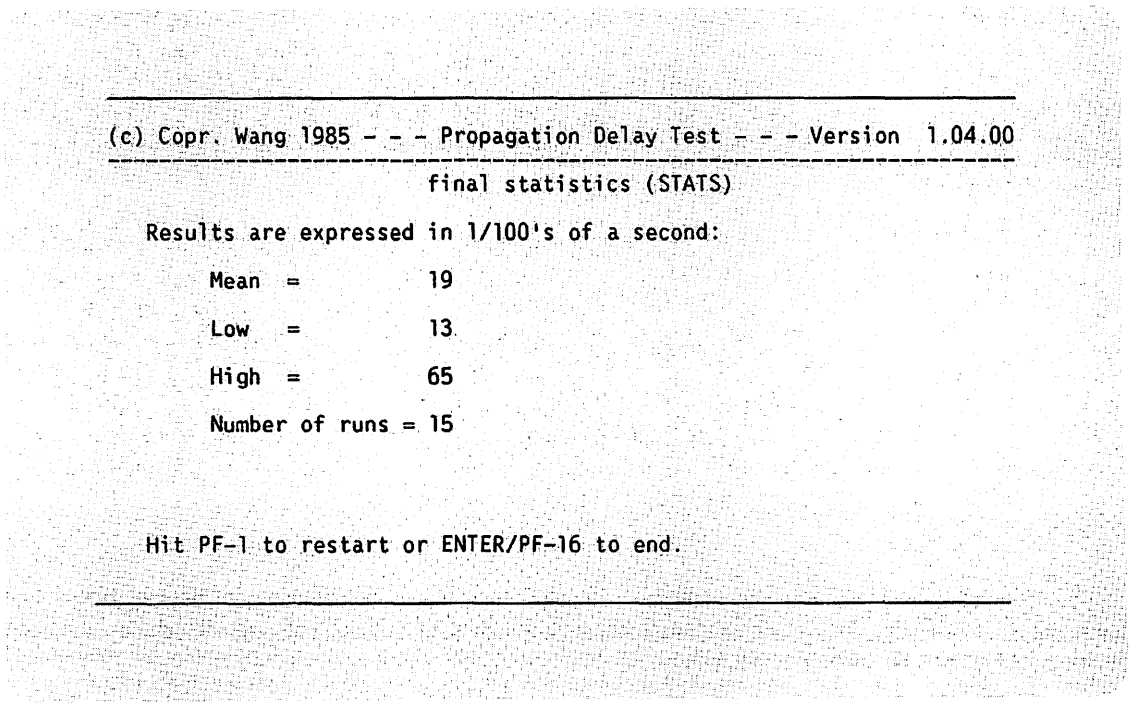

Figure 5-5. PROPTEST Final Statistics Screen

The statistics that PROPTEST gathers during testing are as follows:

Mean -- Displays the average period (in 1/100s of a second) of time it took for a message to travel to the remote system and back.

Low -- Displays the shortest period of time (in 1/100s of a second) it took for a message to travel to the remote system and back.

High -- Displays the longest period of time (in 1/100s of a second) it took for a message to travel to the remote system and back.

Number of runs -- Displays the number of test runs made during testing. If this number is not the same as the number specified on the PROPTEST Parameters screen, an error has occurred during testing.

When you have finished viewing the information on the PROPTEST Statistics screen, press PF1 (Restart) to run PROPTEST again or PF16 (End) to return to the CNS Manager Diagnostics screen. If PF1 is selected, the results of the next execution are appended to the existing log file. If PF16 is selected, the existing log file is deleted the next time the test is run.

USING SYNCHRONOUS SEND/RECEIVE TEST

The Synchronous Send/Receive Test (SYNCTEST) verifies the accuracy of data transferred between two systems. When SYNCTEST is run, messages are sent to PASSTEST at the remote system, which returns each message to the originating system. A comparison is then made, at the originating system, between the messages originally sent and the messages returned. The originating system can detect inconsistencies between the two sets of messages, thereby determining message integrity.

SYNCTEST performs a series of comparisons to determine whether or not messages are formatted correctly and are received in the proper sequence. When a SYNCTEST message is formatted prior to being sent, each byte in the message is numbered. When PASSTEST returns the message to the local system, the bytes must be received in order as originally numbered. For example, bytes labeled 1, 2, and 3 respectively should be received in numerical order. If the bytes are not received in the right order, or if one or more of them is missing, SYNCTEST records the error as a "miscompare."

Note: *Miscompares should never occur. However, miscompares indicate a serious network error, and you should contact your Wang customer representative.*

The messages must also be received in the proper sequence. Each message is uniquely identified by the number of bytes it contains, and is sent to PASSTEST at the remote system in sequence with other messages. All messages must then be returned in the proper sequence.

When you press PF3 on the CNS Manager Diagnostic screen, the SYNCTEST Parameters screen appears (Figure 5-6).

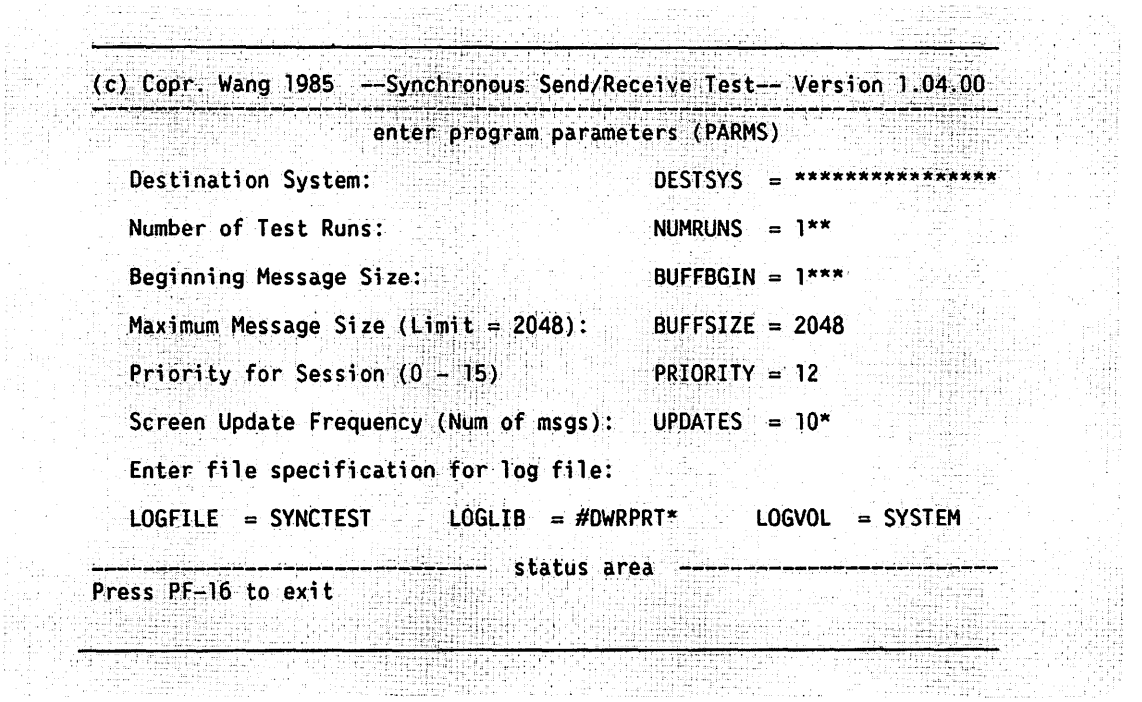

Figure 5-6. SYNCTEST Parameters Screen

The SYNCTEST Parameters screen allows you to enter the parameters that determine the integrity of data transferred between two systems. You must enter these parameters in the fields on the SYNCTEST Parameters screen before SYNCTEST can make test runs. To delete characters from these fields, position the cursor on the character you wish to delete and press DELETE.

Specifying the SYNCTEST Parameters

The following parameter fields appear on the SYNCTEST Parameters screen:

Destination System (DESTSYS) -- Enter the name of the remote system. The name must be one that was defined in the network directory when WSNEDIT was run to define areas and systems in the network (refer to the *VS Network Configuration Guide*).

Note: *If the destination system name is left blank, DESTSYS defaults to the local system.*

Number of Test Runs (NUMRUNS) -- Enter the number of test runs you want SYNCTEST to make. This number will be the number of times SYNCTEST will measure the rate of data transfer between two systems. The valid values for this field range from 1 to 999. The default value is 1.

Note: *The number of times that SYNCTEST measures data integrity is calculated using the formula: (BUFFSIZE Value - BUFFBGIN Value) X NUMRUNS Value = Number of times data integrity is measured.*

Beginning Message Size (BUFFBGIN) -- This field allows you to set the minimum message size to be sent. The valid range of values for this field is 1 to 2048 bytes (2K). The default value is 1.

Maximum Message Size (BUFFSIZE) -- Enter the message size (in bytes) to be allocated to the SYNCTEST session. The message size field indicates the maximum size of the message transmitted to the remote system (via SYNCTEST). The valid values for this field range from 1 to 2048 bytes (2K). The default value is 2048.

Priority for Session (PRIORITY) -- CNS uses priority windows to manage sessions. Sessions with low priority window values are given greater access to the network than sessions with high priority window values. The SYNCTEST test runs tend to be faster if they are assigned low priority window values. The valid values for this field range from 0 to 15. The default value is 12.

Screen Update Frequency (UPDATES) -- Indicates how many messages will be sent (via SYNCTEST) before the SYNCTEST Parameters screen status area is updated. For example, if you enter 1 in this field, SYNCTEST will display the number of every message as it is sent (1, 2, 3, etc.). If you enter the default value 10, SYNCTEST will display the number of every tenth message as it is sent (10, 20, 30, etc.). The valid values for this field range from 1 - 999. The default value is 10.

Note: *Because it takes time for SYNCTEST to update the status area of the screen, frequent screen updating detracts from achievable throughput. To obtain maximum throughput, set the screen update frequency value high.*

LOGFILE -- Enter the name of the VS print file in which SYNCTEST results will be stored. You can use the default name SYNCTEST or specify another file.

LOGLIB -- Enter the name of the library in which you want the log file to reside. You can use the default library (your VS print file library) or specify another valid library.

LOGVOL -- Enter the name of the volume on which your log library resides. The default volume is the system volume.

Running SYNCTEST

Press ENTER when you have specified the parameters required to run SYNCTEST. A series of messages appears on the screen after you press ENTER. These messages provide the following information:

- SYNCTEST is attaching to the network.
- An attempt is being made to open a session with the SYNCTEST program at the remote system.
- The open attempt has succeeded or failed. If the open attempt does not succeed, an error message is displayed that tells you the reason for the open attempt failure. You then must press ENTER to continue. The SYNCTEST Statistics screen appears, allowing you to press PF16 to exit from SYNCTEST or press PF1 to run the program again.
- Test runs are in progress.
- Test runs have been completed and an attempt is being made to close the session with the SYNCTEST program at the remote system. An attempt is also being made to detach from the network.

SYNCTEST Statistics

When SYNCTEST completes the designated number of test runs, the SYNCTEST final statistics screen appears, displaying the statistics gathered during testing. The same screen also appears if the SYNCTEST program at the remote system could not be contacted and ENTER is pressed to continue. Figure 5-7 shows a sample SYNCTEST final statistics screen.

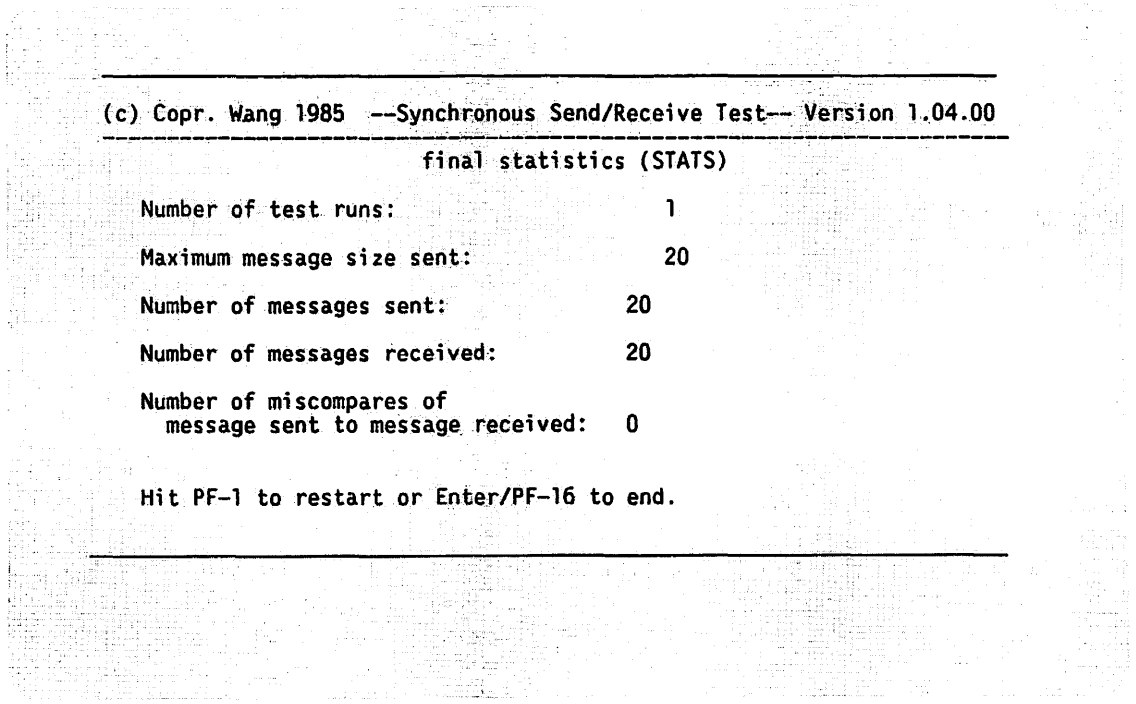

Figure 5-7. SYNCTEST Final Statistics Screen

The statistics that SYNCTEST gathers during testing are as follows:

Number of test runs -- Displays the number of test runs made during testing. If this number is not the same as the number of test runs (NUMRUNS) specified on the SYNCTEST Parameters screen, an error has occurred during testing.

Maximum message size sent -- Displays the value entered in the Maximum Message Size (BUFFSIZE) field on the SYNCTEST Parameters screen. If it does not match, an error has occurred.

Number of messages sent -- Displays the number of messages (i.e., buffers) sent to the remote system. An error has occurred if the value in this field is not as given by the following formula:

(BUFFSIZE Value - BUFFBGIN Value +1) x NUMRUN Value

Number of messages received -- This field should display the same value that is displayed in the Number of messages sent field. If it does not match, an error has occurred.

Number of miscompares of messages sent to messages received -- Displays the number of messages that were received incorrectly. Under normal circumstances, this will always be 0. Any value other than 0 indicates a serious network malfunction, and indicates a need to contact a Wang customer representative.

When you have finished viewing the information on the SYNCTEST Final Statistics screen, you can press PF1 (Restart) to run SYNCTEST again or PF16 (End) to return to the CNS Manager Diagnostics screen. If PF1 is selected, the results of the next execution are appended to the existing log file. If PF16 is selected, the existing log file is deleted the next time the test is run.

USING CONNECT TEST

The CNS Connectivity Test (CONECTST) determines which remote systems in the network can be contacted by the local system. You can specify the systems in the network, or in the local area, that you want CONECTST to contact.

Any systems that you want to contact with CONECTST must be included in the directory file or in a list of network systems in a VS source file. These files are created through WSNEDIT. Refer to the *VS Network Configuration Guide* for information about WSNEDIT.

When you press PF4 on the CNS Manager Diagnostic screen, the CONECTST Parameters screen appears (Figure 5-8).

```
(c) Copr. Wang 1985  - - - CNS Connectivity Test - - -  Version 1.04.02
                          enter program parameters (PARMS)

Enter file specification to use a previously defined file:
RUNFILE  = ********      RUNLIB   = ********      RUNVOL   = ******
Enter file specification for log file:
LOGFILE  = CONECTST      LOGLIB   = #DWRPRT*      LOGVOL   = SYSTEM
Then choose function:
ENTER  Run from above-named file        PF-2  Select from above-named file
PF-3   Run for all systems on network   PF-4  Select from systems on network
PF-5   Run for all systems in area      PF-6  Select from systems in area
PF-16  Exit CONECTST
------------------------  status area  ---------------------------------
```

Figure 5-8. CONECTST Parameters Screen

The CONECTST Parameters screen allows you to specify

- Whether a VS source file or the directory file will contain the list of systems for CONECTST to contact
- The name of the VS source file, if a VS source file is chosen to contain the list of systems that will be included in the test
- The name of the file, library, and volume that will contain the CONECTST statistics when the test is completed

If the list of systems to contact is stored in the directory file, leave the RUNFILE, RUNLIB, and RUNVOL fields blank, and specify the appropriate information in the LOGFILE, LOGLIB, and LOGVOL fields.

If the list of systems to contact is stored in a VS source file, specify the appropriate information in the RUNFILE, RUNLIB, RUNVOL, LOGFILE, LOGLIB, and LOGVOL fields.

You must specify these parameters before running CONECTST.

Specifying the CONECTST Parameters

The CONECTST Parameters screen allows you to specify whether or not the list of systems the local system will attempt to contact is stored in a VS source file or the directory file. If the list of systems is stored in a VS source file, specify the appropriate information in the following fields:

RUNFILE -- Enter the name of the VS source file in which the list is stored.

RUNLIB -- Enter the name of the library in which the VS source file resides.

RUNVOL -- Enter the name of the volume on which the library specified in the RUNLIB field resides.

You specify information in the following fields regardless of your choice of files (VS source or directory):

LOGFILE -- Enter the name of the file in which CONECTST statistics are to be stored. The name defaults to CONECTST. Enter the default setting, or type in a new file name.

LOGLIB -- Enter the name of the library in which the log file will reside. This field defaults to your print file library. Enter the default setting, or type in a new name.

LOGVOL -- Enter the name of the volume on which the log library will reside. The name defaults to the system volume name. Enter the default setting or type in a new value.

Functions on the CONECTST Parameters Screen

Table 5-2 lists the functions on the CONECTST Parameters screen.

Table 5-2. CNS Connectivity Test Screen Functions

When You Press	You Can
PF2 (Select from above-named file)	Contact systems from the list of systems in the VS source file. The entire directory file is read and compared to the VS source file. The systems in the VS source file are then preselected.
PF3 (Run for all systems on network)	Contact all the systems in the network defined in the directory file.
PF4 (Select from systems on network)	Contact selected systems from the list of systems in the network defined in the directory file. These systems appear on the CONECTST Choose Systems To Test screen.
PF5 (Run for all systems in area)	Contact all the systems in your area defined in the directory file.
PF6 (Select from systems in area)	Contact selected systems in your area defined in the directory file. These systems appear on the CONECTST Choose Systems To Test screen.
PF16 (Exit CONECTST)	Return to the CNS Manager Diagnostics screen.
ENTER (Run from above-named file)	Contact all systems specified in the VS source file.

If you press PF key 2, 4, or 6, the Choose Systems To Test screen appears (Figure 5-9). If you press ENTER, PF3, or PF5 from the CONECTST Parameters screen, the CONECTST Results screen appears (Figure 5-10).

```
(C) Copr. Wang 1985 --- CNS CONECTIVITY TEST ---      Version  1.04.02
                    Choose systems to test (SYSTEMS)

Select systems in network

Mark desired systems with an 'X', and press ENTER to test,
  X ATLAS             _ BSSPC1
  _ DENSYS2           X DMR
  _ EEYORE            _ ENDPOINT
  _ JMALLNC           _ NEWYORK1
  _ BOSTON1           _ NETMGMT
  _ OFM1              _ OFM2
  _ OS2               _ PC1
  _ PC4               _ PC5
  _ PCVS90            X PROBE
  _ QASERVER          _ QAVS


                                                PF-8    Find system
PF-3 Last     PF-5 Next Screen                  PF-16   Exit CONECTST
 ------------------------ status area ------------------------------
```

Figure 5-9. Choose Systems To Test Screen

The Choose Systems To Test screen allows you to select individual systems from a list of systems. If you pressed PF2 from the CONECTST Parameters screen, the systems in the VS source file that correspond to systems in the directory file are marked with an X. If you pressed PF4 from the CONECTST Parameters screen, the list is read from the directory file and comprises all the systems in the network. If you pressed PF6 from the CONECTST Parameters screen, the list is read from the directory file and comprises all the systems in the local system's area.

Type X next to each system that you want to contact. If an X already exists next to a system that you do not want to contact, position the cursor on that X and press the space bar or DELETE to remove it.

Functions on the Choose Systems To Test Screen

Table 5-3 lists the available functions on the Choose Systems To Test Screen.

Table 5-3. Choose Systems To Test Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next Screen)	Scroll through the list of systems when the list consists of more than one screen.
PF8 (Find System)	Enter the name of a specific system that you want to include in the test. The System Name prompt appears at the base of the screen. Type the name of the desired system, and press ENTER to accept the selection, or PF16 to return to the CONECTST Choose Systems To Test screen. When the name of the specified system is displayed on the screen, you can choose it to be included in the test. ***Note:*** *No leading or embedded blank spaces are allowed in this field. If the system name that is entered contains any blanks, the screen will display the message "Remove leading or embedded blanks."*
PF16 (Exit CONECTST)	Terminate CONECTST.
ENTER	Display the CONECTST Results screen.

Displaying CONECTST Results

Press ENTER when you have finished selecting and/or deleting systems from the Choose System To Test screen. The CONECTST Results screen appears (Figure 5-10).

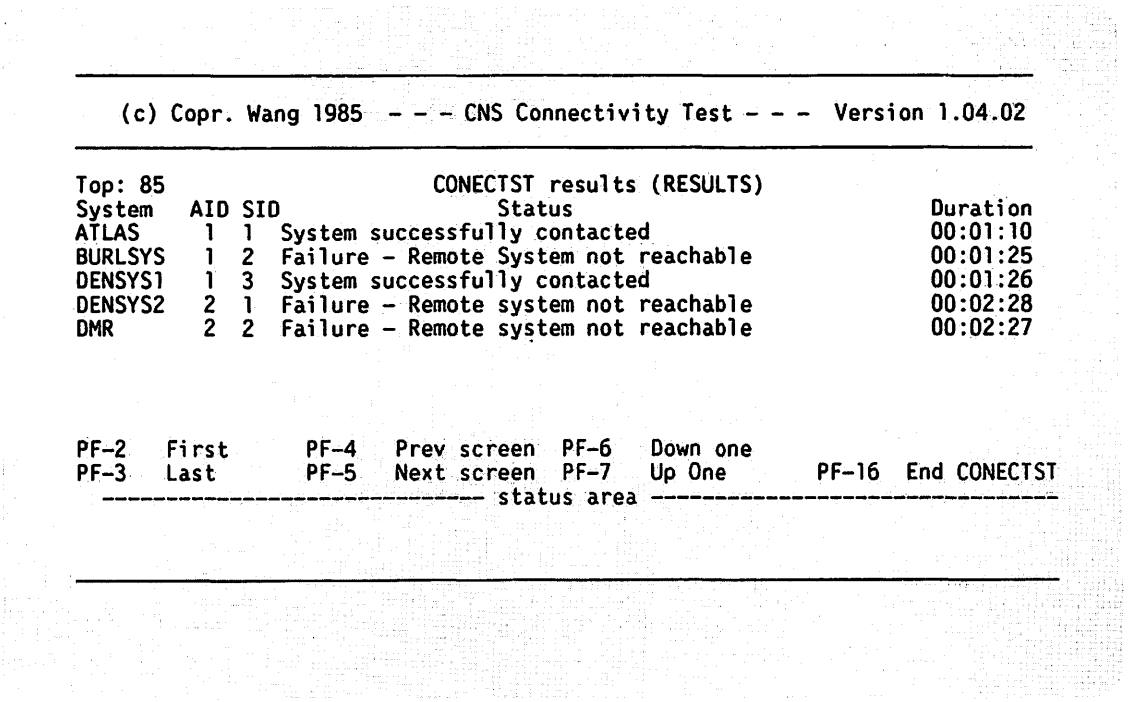

Figure 5-10. CONECTST Results Screen

The CONECTST Results screen lists the names, area IDs, and system IDs of all the systems that the local system is attempting to contact. The screen also lists the status of CONECTST's attempt to contact each system. When CONECTST initially attempts to contact remote systems, the message "Initial - Connection attempt beginning" appears in the Status column for each system. This message is eventually replaced by "Open Sent - Waiting for response."

For remote systems that cannot be contacted, a message appears in the Status column for each system explaining why contact is not possible. Refer to the appendix on CNS Log Messages and Reason Codes for an explanation of these messages. For remote systems that can be contacted, a message appears indicating that the system has been successfully contacted.

When a message indicating whether or not a system can be contacted appears, the amount of time it took to attempt to contact that system appears in the Duration field.

Note: *When CONECTST is running, you can cancel the program by pressing HELP, and then PF16.*

Functions on the CONECTST Results Screen

When CONECTST has concluded testing, several PF keys appear at the bottom of the CONECTST Results screen. Table 5-4 lists the available functions.

Table 5-4. CONECTST Results Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next Screen)	Scroll through the list of systems when the list consists of more than one screen.
PF6 (Down One)	Scroll down one line.
PF7 (Up One)	Scroll up one line.
PF16 (End CONECTST)	Displays the CONECTST Statistics screen.

Displaying the CONECTST Statistics

When you press PF16 from the CONECTST Results screen, the CONECTST Statistics screen appears (Figure 5-11). The CONECTST Statistics screen displays the statistics gathered during testing. If systems were read from a VS source file during CONECTST and if a system in the VS source file did not correspond to a system in the directory file, a message appears on the CONECTST Statistics screen indicating that the source file should be replaced.

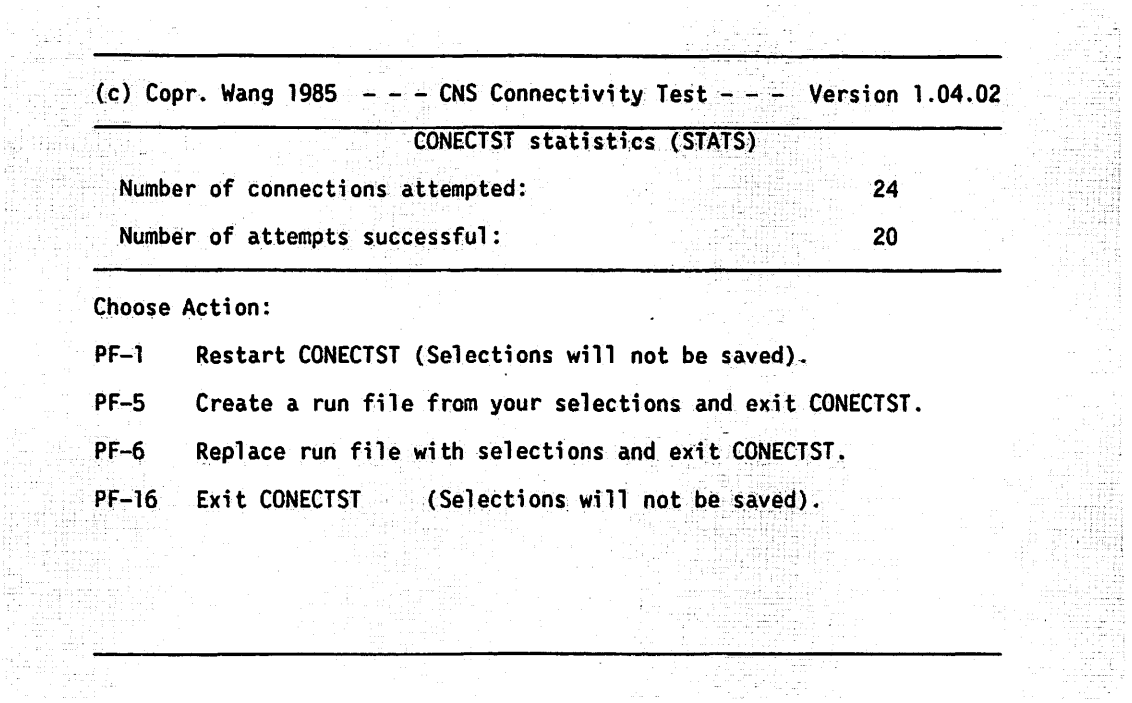

Figure 5-11. CONECTST Statistics Screen

The statistics gathered during CONECTST testing are as follows:

Number of connections attempted -- Displays the number of remote systems CONECTST attempted to contact. CONECTST made one connection attempt to contact each system.

Number of attempts successful -- Displays the number of systems that were contacted successfully.

CONECTST Statistics and Options Screen Functions

Table 5-5 describes the function keys that appear on the CONECTST Statistics screen.

Table 5-5. CONECTST Statistics Screen Functions

When You Press	You Can
PF1 (Restart CONECTST)	Run CONECTST again. The CONECTST Parameters screen appears when you press PF1.
PF5 (Create a run file)	Create a run file to store the list of systems you attempted to contact. If you press PF5, a screen appears that asks you to specify the file in which the list of systems is to be saved. CONECTST will automatically create the file once it is specified. You also must specify an existing library and volume in which the file will reside. Press ENTER once you have specified the file, library, and volume, or press PF1 to cancel the save operation. Pressing ENTER or PF1 returns you to the CONECTST Statistics screen.
PF6 (Replace run file)	Replace the source file with a new file consisting of a list of systems you selected on the CONECTST Select Systems screen. PF6 appears only if CONECTST attempted to contact systems listed in a VS source file. If PF6 is pressed, a screen appears that asks you to specify the file in which the list of systems is to be saved. CONECTST will automatically create the file once it is specified. You must also specify an existing library and volume in which the file will reside. Press ENTER once you have specified the file, library, and volume, or press PF1 to cancel the save operation. Pressing ENTER or PF1 returns you to the CONECTST Statistics and Options screen.

(continued)

Table 5-5. CONECTST Statistics Screen Functions (continued)

When You Press	You Can
PF16 (Exit CONECTST)	Go to the CNS Manager Diagnostics screen. This allows you to exit from CONECTST without saving the list of systems that CONECTST attempted to contact. When you press PF16, a warning message appears on the screen. This message prompts you to press PF1 if you want to save the list, or press PF16 to exit without saving the list. If you press PF1, the CNS CONECTST Parameters screen appears. You can then press the appropriate PF key to save the list. If you press PF16 to terminate CONECTST without saving the list of systems that CONECTST attempted to contact, the CNS Diagnostics menu appears.

USING PATH TRACE

Path Trace is a routing diagnostic tool that allows you to trace the logical path that a data message will take from the local system to a specified destination system. When you select a destination system and then submit a path trace, the local VS system sends a path trace message to the destination system. The path trace collects information on all the systems and transports along the path before routing the path trace results back to the local system. The results include all the systems in the path, as well as the status (success or failure) of each link along the path. You can also display detailed path trace results between any pair of systems in the trace path. Path Trace allows you to identify network problems, such as system and transport failures, that are currently inhibiting efficient routing between your local system and a destination system.

When you select PF5 (Path Trace) on the CNS Manager Diagnostics menu, the path trace file is read. The path trace file contains the latest path trace statistics for each system. After the path trace file is read, the Path Trace screen appears. Figure 5-12 shows a sample Path Trace screen.

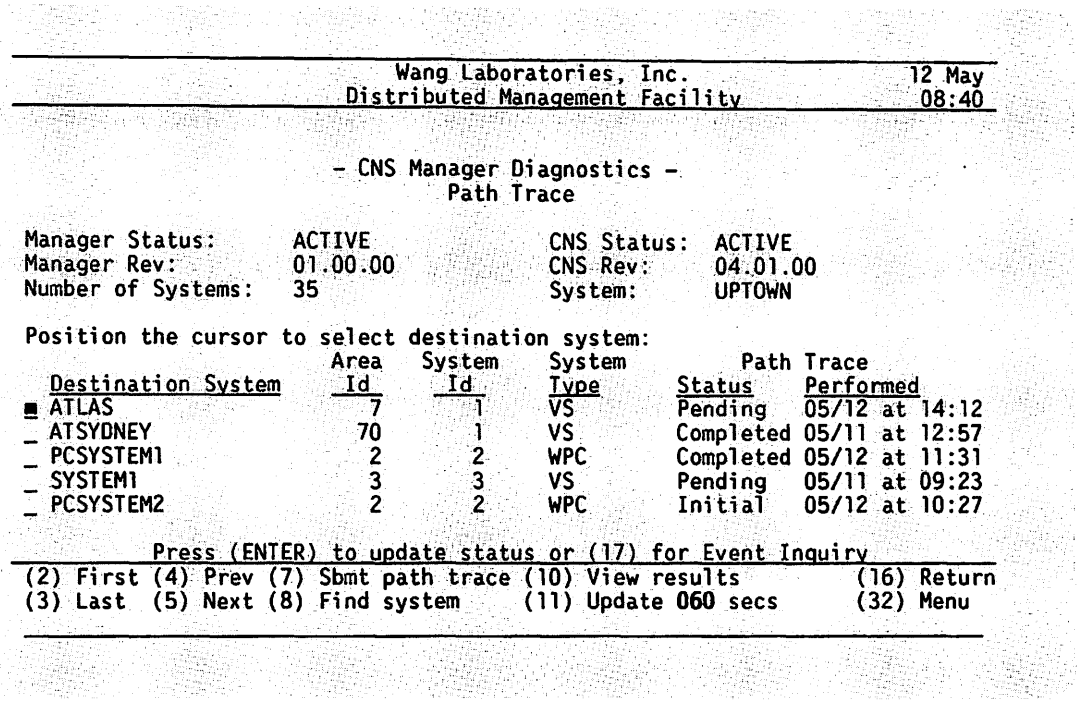

Figure 5-12. Path Trace Screen

The Path Trace screen displays the statistics (acquired from the most recent path trace) on the destination systems.

The following fields appear on the Path Trace screen:

Manager Status -- The current state of the CNS Manager background task at the local system. If you do not have the Distributed Management Facility, the status is always ACTIVE.

CNS Status -- The current status of CNS on the local system. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE, you can stop CNS by pressing PF2 from the CNS Manager Summary Status screen.

INACTIVE -- If the CNS status is INACTIVE, you can start CNS by pressing PF1 from the CNS Manager Summary Status screen.

TIMEOUT -- The CNS Manager has sent a message to CNS, but no response has been received.

Manager Rev -- The version of the CNS Manager currently running on the local system.

CNS Rev -- The current version of CNS on the local system.

Number of Systems -- The number of destination systems that can be contacted by the local system, as configured through WSNEDIT.

System -- The name of the local system; that is, the system onto which you are logged.

Destination System -- The name of the destination system in the local view directory file defined by WSNEDIT.

Area Id -- The area ID of the destination system, as defined in the directory file by WSNEDIT.

System Id -- The system ID of the destination system, as defined in the directory file by WSNEDIT.

System Type -- The type of CNS system: VS, WPC, PC, or IBM.

Path Trace Status -- The status of the last path trace that was submitted, as follows:

Completed -- Path trace results have been received for this entry.

Initial -- No path trace attempt has been made to the remote system.

Lost -- A trace was submitted but the path trace timer expired before completion. The path trace is considered lost at this point.

Pending -- A path trace has been submitted for this entry and has not yet come back.

Path Trace Performed -- The date and time of the path trace.

Functions on the Path Trace Screen

Table 5-6 describes the function keys that appear on the Path Trace screen.

Table 5-6. CNS Manager Path Trace Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of systems when the list consists of more than one screen.
PF7 (Submit path trace)	Submit a path trace to the selected destination system. ***Note:*** *The destination system must be selected before the path trace can be submitted. Select the destination system by positioning the cursor next to the system name, and then press PF7 to submit the path trace.*
PF8 (Find system)	Enter the name of a specific system to display the screen containing this system. The System Name prompt appears at the base of the screen. Type the name of the desired system, and press ENTER to accept the selection or PF16 to return to the Path Trace screen. ***Note:*** *No leading or embedded blank spaces are allowed in this field. If the system name that is entered contains any blanks, the screen will display the message "Remove leading or embedded blanks."*
PF10 (View Results)	View the results of a completed path trace.
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 - 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Manager Diagnostics menu.

(continued)

Table 5-6. CNS Manager Path Trace Screen Functions (continued)

When You Press	You Can
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS status information.

Submitting the Path Trace and Displaying the Results

When you display the Path Trace screen, you must select the destination system before submitting the path trace. Select the destination system by positioning the cursor next to the system name, and then press PF7 to submit the path trace.

When the path trace completes, press PF10 (View Results) to display the Path Trace Results screen (Figure 5-13).

```
                          Wang Laboratories, Inc.                    12 May
                        Distributed Management Facility              08:40

                          - CNS Manager Diagnostics -
                              Path Trace Results

Manager Status:       ACTIVE              CNS Status:  ACTIVE
Manager Rev:          01.00.00            CNS Rev:     04.01.00
Performed By:         JPD                 System:      UPTOWN
Date/Time Performed:  05/12 at 12:57      Destination: ATLAS

Position cursor on desired results and press (10) for more detail:

  Send From System  To System    Using Transport  Status   Rejected By
_ UPTOWN            LOCALNET     WANGBANDLINK1    Success
_ LOCALNET          COMET        WANGPAC          Failure  Transport
_ LOCALNET          ATLAS        WANGNET          Success
_ ATLAS             COMET        WANGPAC          Failure  Sender
_ ATLAS             LOCALNET     WANGBAND         Success
        Press (ENTER) to update status or (17) for Event Inquiry
                                  (10) Detailed results      (16) Return
(3) Last  (5) Next                (11) Update 060 secs       (32) Menu
```

Figure 5-13. Path Trace Results Screen

The Path Trace Results screen displays all of the systems currently required to reach the destination system. If a failure occurs between two systems, the sending system attempts to connect to another system. The process continues until a path to the destination system is found, all possible paths are exhausted, or a timer has expired.

The following fields appear on the Path Trace Results screen:

Manager Status -- The current state of the CNS Manager background task at the local system. If you do not have the Distributed Management Facility, the status is always ACTIVE.

CNS Status -- The current status of CNS on the local system. The CNS status can be

ACTIVE -- If the CNS status is ACTIVE, you can stop CNS by pressing PF2.

INACTIVE -- If the CNS status is INACTIVE, you can start CNS by pressing PF1.

TIMEOUT -- The CNS Manager has sent a message to CNS, but no response has been received.

Manager Rev -- The version of the CNS Manager currently running on the local system.

CNS Rev -- The current version of CNS on the local system.

Performed By -- The logon ID of the user conducting the path trace.

System -- The name of the local system; that is, the system onto which you are logged.

Date/Time Performed -- The time and date when the path trace was submitted.

Destination -- The name of the destination system to which you are tracing a path.

Send From System -- The name of the system that initiated a path trace.

To System -- The name of the system receiving the path trace.

Using Transport -- The name of the transport connecting the system pair.

Status -- The path trace status of the system pair. The path trace status can be either Success or Failure.

Rejected By -- Indicates the component (sending system or transport) that rejected the path trace.

Functions on the Path Trace Results Screen

Table 5-7 describes the function keys that appear on the Path Trace Results screen.

Table 5-7. CNS Manager Path Trace Results Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last) PF4 (Prev) PF5 (Next)	Scroll through the list of systems when the list consists of more than one screen.
PF10 (Detailed Results)	View the detailed results for any two systems in the trace path.
PF11 (Update ___ secs)	Specify how frequently the screen is automatically updated with current status from CNS. The valid values for this field range from 0 to 999. If 0 or no time is entered, automatic screen updating is disabled. Values that change are highlighted.
PF16 (Return)	Return to the CNS Path Trace screen.
PF17 (Event Inquiry)	Monitor the real-time network messages as they are logged by the LOGTSK program on your local system.
PF32 (Menu)	Return to the CNS Manager Summary Status screen.
ENTER	Update the CNS status information.

Displaying Detailed Path Trace Results

From the Path Trace Results screen, you can obtain detailed path trace information for any system pair. You display detailed path trace information by selecting the system pair and pressing PF10. Figure 5-14 shows a Detailed Path Trace Results screen.

The Detailed Path Trace Results screen displays system configuration and transport information, as well as the reason for a path trace failure between a system pair. Using this information, you can reconfigure transports and routing records (through WSNEDIT) for more efficient routing from your local system to a destination system.

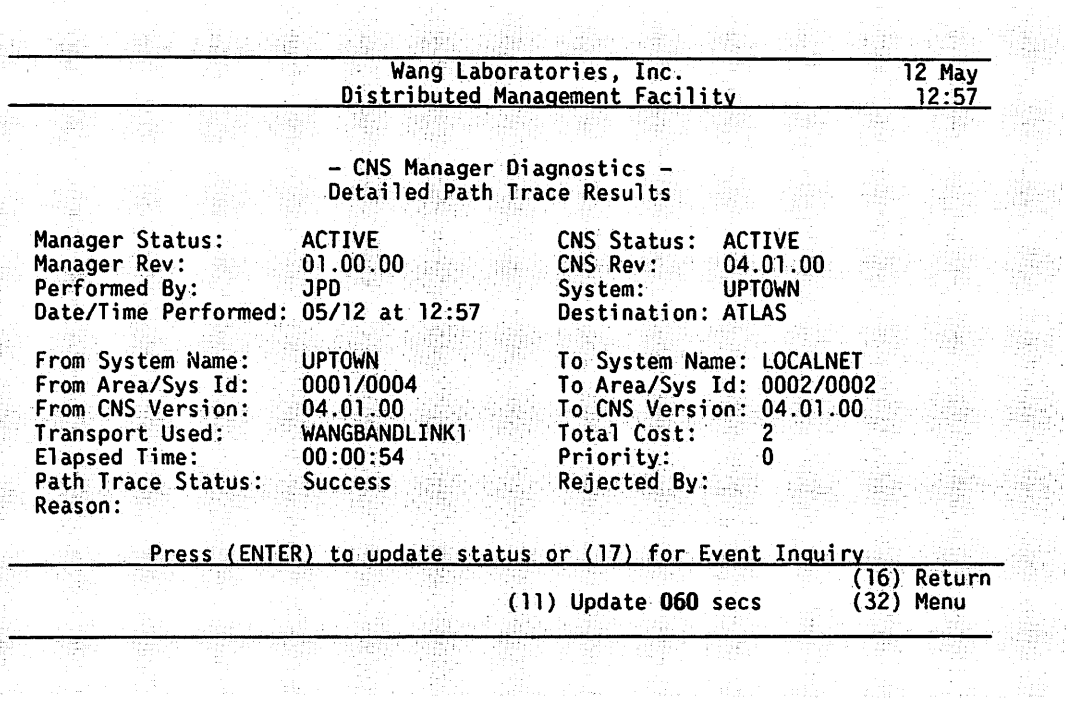

Figure 5-14. Detailed Path Trace Results Screen

The following status fields appear on the Detailed Path Trace Results screen:

From System Name -- The name of the system that initiated a path trace.

To System Name -- The name of the system receiving the path trace.

From Area/Sys Id -- The area ID and the system ID of the system that initiated the path trace.

To Area/Sys Id -- The area ID and the system ID of the system receiving the path trace.

From CNS Version -- The CNS revision level on the system initiating the path trace.

To CNS Version -- The CNS revision level on the system receiving the path trace.

Transport Used -- The name of the transport linking the system pair.

Total Cost -- The transport's total cost, based on the calculation BASE COST + CONGESTION LEVEL.

Elapsed Time -- The duration of the path trace.

Priority -- The priority level that CNS assigns to the path trace task. The priority can be a value from 0 through 15, with 0 being the highest priority.

Path Trace Status -- Indicates path trace FAILURE or SUCCESS.

Rejected By -- The component (sending system or transport) that rejected the path trace.

Reason -- The CNS reason message for a path trace failure. The possible CNS path trace reason messages are

802.3 controller failure
802.3 controller has no buffers
ADD LSAP error
Can't determine sender
Configuration error
Connect error
Destination not active on LAN
Feature not supported
Inactive route
Inactive transport
Initialization error
Invalid LSAP address
Invalid protocol
Invalid protocol command
Invalid transport ID
Lost message (zero hop count)
LSAP not currently active
LSAP previously defined
LSAP table full
Media transmission failure
MLTC error
Next hop not reachable
No active path
No alternate path exists
No available path
No available route
No LSAP in configuration records
No path exists
No routing information available
System directory error
System not defined in directory

System not in name table
System restarted
Transport disabled
Transport table limit exceeded
Transport reset
Unacceptable CNS revision level
Undeliverable

USING CNS TRACE

The CNS Trace function displays the current status of the trace point table. The trace point table is a debugging tool that identifies CNS program modules that exchange internal messages using specific protocols. These messages travel between the various layers of CNS. If the tracing facility is activated, the first 56 bytes of each message that a CNS module sends or receives are stored at a memory address that can be viewed through VS Debugger, or in a CNS task dump.

The CNS Trace function also allows you to enter internal CNS messages to a log file stored on disk. When one module sends a message to another, the entire message is stored in this log file.

You can specify the log volume name and the number of records to be stored in the log file on the CNS Trace Log Settings screen. The library name is always @CNSLOG@. The log file name is CNSLOGXX, where XX is a value from 00 to 99. When you modify the trace points, the volume name, or the number of records, the log file name is incremented by 1. For example, if the latest log file is named CNSLOG53, any modifications that you make change the log file name to CNSLOG54. When the log file name reaches CNSLOG99, the counter starts again with CNSLOG00.

Note: *The CNS Trace function is useful only to qualified Wang personnel with a knowledge of CNS internals.*

When you press PF6 on the CSN Manager Diagnostics screen, the CNS Trace screen appears (Figure 5-15).

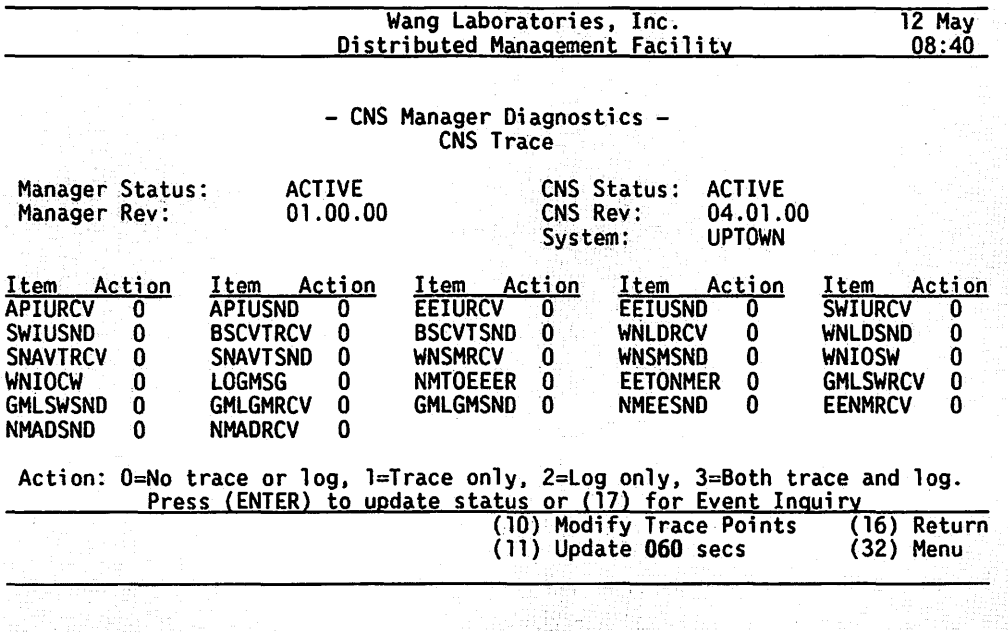

Figure 5-15. CNS Trace Screen

Modifying the Trace Point Table

The CNS Trace screen lists all the CNS modules in the Item columns. The Action columns list fields that allow the user to specify the action to be taken to monitor a module. To specify an action to be taken on a module, press PF10. All the action fields appear in modify (highlighted) mode. You then enter the appropriate action codes next to the module or modules you want to monitor and press ENTER. The following listing describes the action codes and their meanings:

0 (NO TRACE OR LOG) -- No action will be taken to monitor the module.

1 (TRACE ONLY) -- Only a trace will be performed to monitor messages sent from or received by a module. When a trace is performed, you can view the address in memory where the first 56 bytes of a message sent from or received by a module are stored by using the VS debugger or terminating CNS and requesting a dump file.

2 (LOG ONLY) -- Messages only get logged (no trace) to a log file in library @CNSLOG@ on the system volume (or specified volume if NETCORE 8.32 is installed).

3 (BOTH TRACE AND LOG) -- Messages will be both traced and logged.

Notes: *Entering action code 2 or 3 (i.e., enabling either log only or trace and log) may adversely affect CNS performance.*

If you are using a release of WSN VS NETCORE prior to 8.32, the trace points will be turned off when the CNS task is restarted.

If you are using WSN VS NETCORE 8.32 or greater, trace points that are activated will remain activated between executions of the CNS task.

If you are using WSN VS NETCORE 8.32 or greater, and you select action code 2 or 3 and press ENTER, the Modify CNS Trace Log Settings screen will appear. You must specify the file size and volume name for the CNS Trace Log file on the Modify CNS Trace Log Settings screen (Figure 5-16).

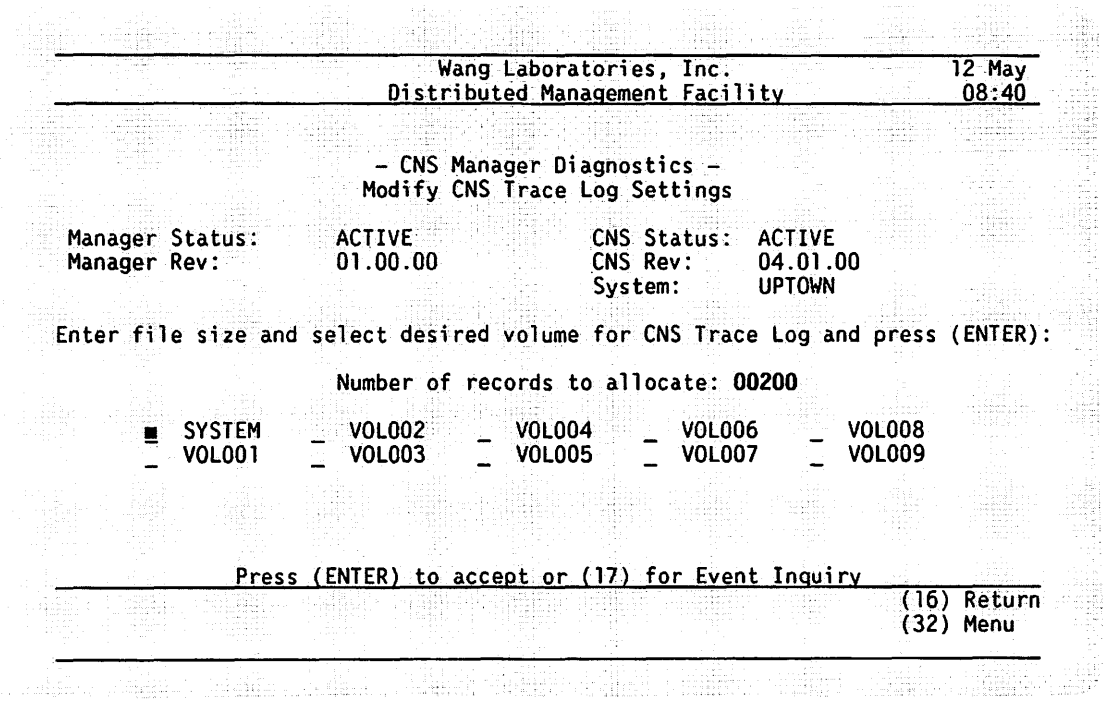

Figure 5-16. Modify CNS Trace Log Settings Screen

CHAPTER 6
VS OPERATIONAL CONTROL

OVERVIEW

This chapter describes the network features listed on the VS Operator's Console menu. The VS Operator's Console allows you to control and monitor network communications activity with the following functions:

PF4 (Transmit Queue) -- Allows you to control and monitor the files that are awaiting transmission from your local system to remote systems

PF5 (Retrieve Queue) -- Allows you to control and monitor the files that are awaiting retrieval from remote systems

PF6 (Interactive Tasks) -- Allows you to control and monitor the programs that are currently running on your local system

PF12 (Telecommunications) -- Allows you to control and monitor links, devices, systems, and services

PF13 (Workstations) -- Allows you to control and monitor the workstations on your local system

To access the VS Operator's Console, press PF11 (Enter Operator Mode) on the VS Command Processor menu.

CONTROLLING THE TRANSMIT AND RETRIEVE QUEUES

The transmit queue and retrieve queue are lists of files that have been queued for transfer between the local system and a remote system. The queues are generated from the VS TRANSFER utility. The VS transmit queue lists all files awaiting transmission from your local system to the remote system. The VS retrieve queue lists all files awaiting retrieval from the specified remote system.

You can perform a variety of operations from the transmit and retrieve queues:

- Displaying the files that have been queued through the TRANSFER utility
- Displaying the destination and status of each file on the queue
- Removing a file from the queue
- Stopping a file transfer that is in progress
- Changing the status of a file on the queue from Hold to Active or from Active to Hold
- Displaying the name, library, and volume of the file on the local system
- Displaying the name, library, and volume of the file on the remote system

Your local users are the initiators of all requests on these queues. For each request on either queue, the Status column indicates "Xfering" if the transfer is in progress, "Hold" if the request is suspended, or a blank status for a request actively awaiting transfer.

Transmit Queue -- Local Information

The transmit queue lists all files that have been queued for transfer from the local VS system for printing or storage on a remote system. To display the VS Transmit Queue screen (Figure 6-1), press PF4 from the VS Operator's Console menu.

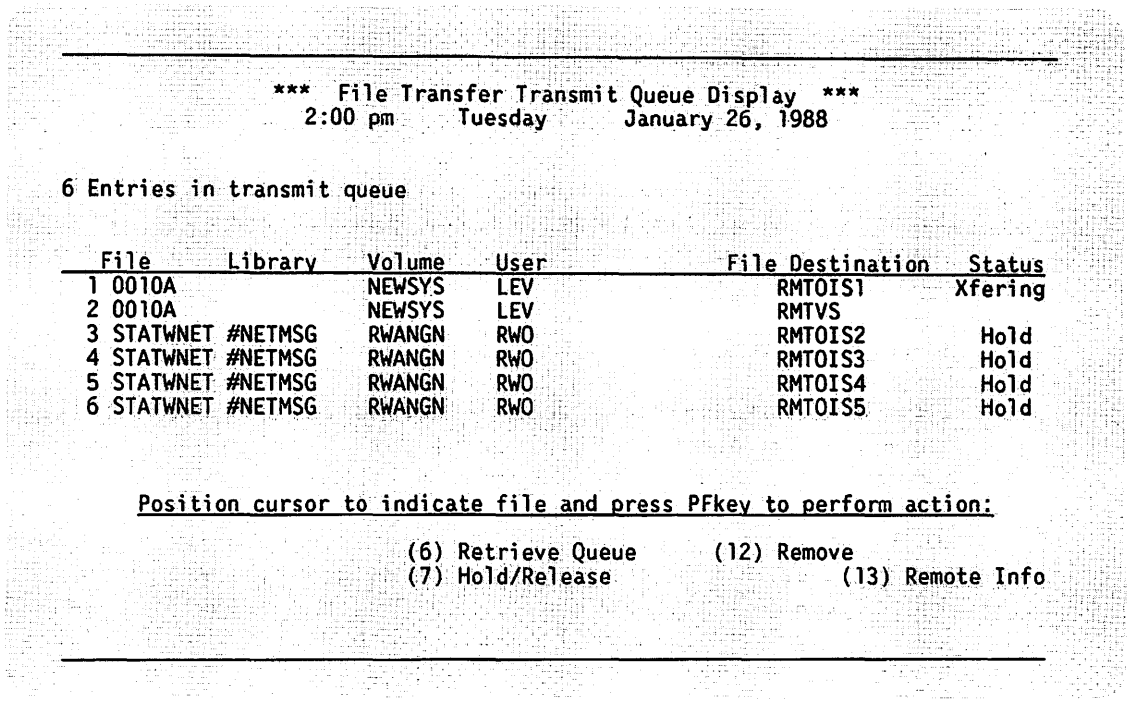

Figure 6-1. Sample VS Transmit Queue Screen -- Local Information

The VS Transmit Queue screen displays the following local information:

File -- The file name or document ID of the file/document that is currently being sent or waiting to be sent.

Library -- The name of the VS library that contains the transfer file. No library is displayed for a document.

Volume -- The name of the VS volume that contains the file/document that is being sent.

User -- The ID of the VS user who initiated the transfer.

File Destination -- The name of the system that will receive the file or document.

Status -- The current status of the document or file on the queue. Hold indicates that the file will not be transmitted until it is released. Xfering indicates that the file or document is currently being transmitted to the remote system. A blank indicates that the file or document is in active status and will be transmitted without any operator intervention when it reaches the top of the queue.

Transmit Queue Screen Functions

The following functions are available from the VS Transmit Queue menu:

PF2 - PF5 -- Scrolls through multiscreen queues. PF2 displays the first screen of the queue, PF3 the last screen, PF4 the screen previous to the current one, and PF5 the screen after the current one.

PF6 (Retrieve Queue) -- Displays the retrieve queue.

PF7 (Hold/Release) -- Places an active request on hold (the status changes from blank to Hold) or places a hold request on the active waiting list (the status changes from Hold to blank).

PF12 (Remove) -- Removes the selected request from the queue. (This action does not delete the file or document.) A system administrator can remove a request, if the queue is accessed through PF12 (Telecommunications) on the Operator's Console screen. If the queue is accessed through the Command Processor, the file owner is the only person who can remove the request.

PF13 (Local/Remote Information) -- Displays the local or remote form of the queue. The remote form of the transmit queue contains a column labeled Transfer Group. You must assign the transfer group to the request. The transfer group must be defined on the destination system (your system if a file is being retrieved, or the remote system if the file is being sent).

Transmit Queue -- Remote Information

The transmit queue provides information only on those files or documents that have been queued from the local VS. The Remote Information screen (PF13) provides information on these same files or documents as they appear on the remote system. Figure 6-2 shows a sample VS Transmit Queue Remote Information screen.

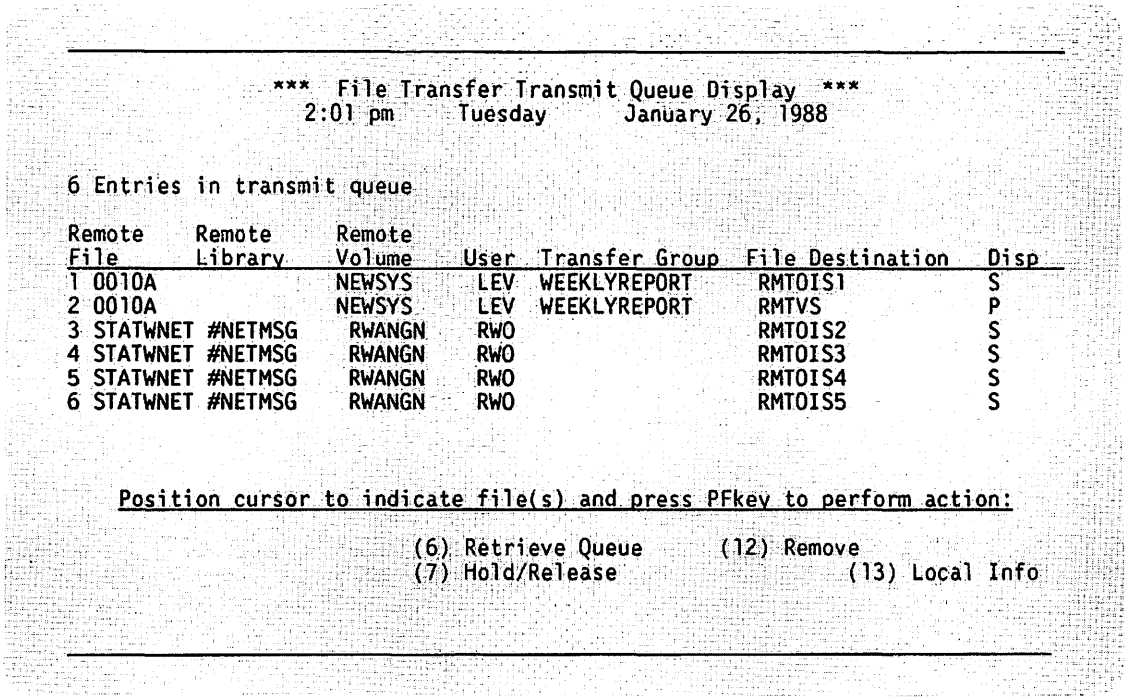

Figure 6-2. Sample VS Transmit Queue Screen -- Remote Information

The Remote Information screen displays the following information:

Remote File -- The file name or document ID that the file/document will have when it is transferred to the receiving system. <PRINT> indicates that the file will be entered into the print queue of the receiving system. You can transfer the file or document to the remote system for printing, and then have the remote system retain the file or document after printing.

Remote Library -- The name of the library on the receiving system that will store the file being sent.

Remote Volume -- The name of the volume on the receiving system that will store the transferred file or document.

User -- The logon ID of the user who has initiated a file transfer.

Transfer Group -- The name of the transfer group on the remote system to which the file or document will be assigned.

File Destination -- The name of the destination system to which the file is being sent.

Disp -- The disposition of the file or document on the receiving system. S indicates that the file will be stored; P indicates that the file will be printed. If you choose to store the file or document after printing, the disposition is still listed as P.

Retrieve Queue -- Remote Information

The retrieve queue lists all files and documents that have been queued for retrieval from a remote system for printing or storage on the local VS system. Press PF5 from the VS Operator's Console menu to display the VS Retrieve Queue screen (Figure 6-3).

```
*** File Transfer Retrieve Queue Display ***
  2:03 pm      Tuesday      January 26, 1988

1 entry in retrieve queue

Remote File  Remote Library  Remote Volume  User  File Origin  Status
REP0002      Q3REPS          PRODUCTS       REB   BOSTON       Xfering

Position cursor to indicate file and press PFkey to perform action:

(6) Transmit Queue      (12) Remove
(7) Hold/Release              (13) Local Info
```

Figure 6-3. Sample VS Retrieve Queue Screen -- Remote Information

The Retrieve Queue screen displays the following remote information:

Remote File -- The file name or document ID of the file/document on the remote system.

Remote Library -- The name of the library on the remote system that contains the file/document to be retrieved.

Remote Volume -- The name of the volume on the remote system that contains the file/document to be retrieved.

User -- The ID of the VS user who initiated the transfer.

File Origin -- The name of the remote system from which the file/document will be retrieved.

Status -- The current status of the document/file on the queue. Hold indicates that the file will not be retrieved until it is released. Xfering indicates that the file/document is currently being retrieved from the remote system. A blank indicates that the file/document is in active status and will be retrieved without any operator intervention when it reaches the top of the queue.

Retrieve Queue Screen Functions

The Retrieve Queue screen contains the following functions:

PF2 - PF5 -- Scrolls through multiscreen queues. PF2 displays the first screen of the queue, PF3 the last screen, PF4 the screen previous to the current one, and PF5 the screen after the current one.

PF6 (Transmit Queue) -- Displays the transmit queue.

PF7 (Hold/Release) -- Places an active request on hold (the status changes from blank to Hold) or places a hold request on the active waiting list (the status changes from Hold to blank).

PF12 (Remove) -- Removes the selected request from the queue. (This action does not delete the file or document.) A system administrator can remove a request if the queue is accessed through PF12 (Telecommunications) on the Operator's Console screen. If the queue is accessed through the Command Processor, the file owner is the only person who can remove the request.

PF13 (Local/Remote Information) -- Displays the local or remote form of the retrieve queue. The local form of the retrieve queue contains a column labeled Transfer Group. You must assign the transfer group to the request. The transfer group must be defined on the destination system (your system if a file is being retrieved, or the remote system if the file is being sent).

Retrieve Queue -- Local Information

When you press PF13 (Local info), the VS Retrieve Queue Local Information screen appears (Figure 6-4). This screen displays information on the files and documents as they appear on the local system.

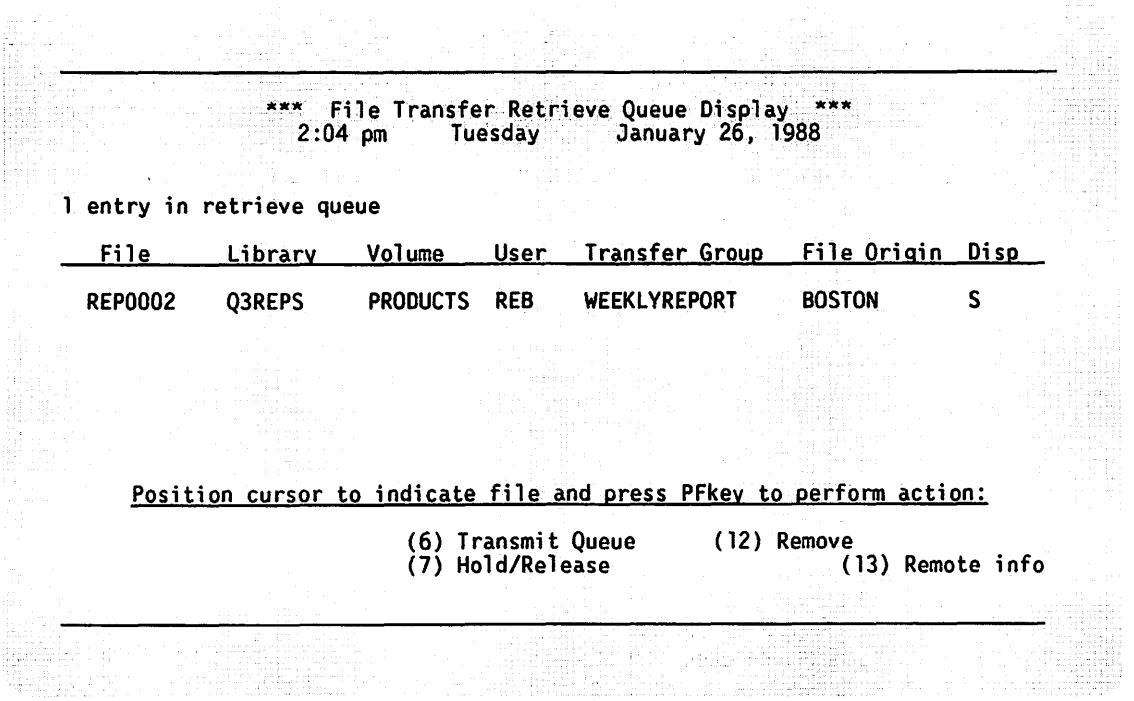

Figure 6-4. Sample VS Retrieve Queue Screen -- Local Information

The Local Information screen displays the following information:

File -- The file name or the document ID to be assigned to the file/document when it is received. This field is blank if you did not specify the file name or document ID in the TRANSFER utility.

Library -- The name of the VS library that has been designated to receive the retrieved file. No library is displayed for a document.

Volume -- The name of the VS volume that will contain the file/document when it is received.

User -- The ID of the VS user who requested the transfer.

Transfer Group -- The name of the transfer group on the local system to which the file or document will be assigned.

File Origin -- The name of the remote system from which the file or document will be retrieved.

Disp -- The disposition of the file or document on the local VS. S indicates that the file will be stored; P indicates that the file will be printed. If you choose to store the file or document after printing, the disposition is still listed as P.

CONTROLLING INTERACTIVE PROCESSING TASKS

The Control Interactive Tasks menu displays information about all interactive tasks running on your local system. An interactive task is any job or procedure requiring ongoing communication with a VS user. The system treats all workstations as interactive tasks.

When you press PF6 at the VS Operator's Console, you can perform operations that allow you to control and monitor interactive tasks. These operations include

- Examining the status and time statistics of the interactive tasks
- Examining the paging and I/O statistics of the interactive tasks
- Accessing the Control Non-Interactive Tasks menu
- Monitoring the program status of an interactive task
- Changing the status of an interactive task
- Canceling an interactive task
- Controlling user logon or logoff for one workstation
- Controlling user logon or logoff for all workstations

To perform any of these operations, press PF6 from the Operator's Console menu. The Control Interactive Tasks (Status and Time) screen appears (Figure 6-5).

*** Control Interactive Tasks (Status and Time) ***
2:07 pm Tuesday January 26, 1988

5 interactive tasks in system

WS	User	Status	Program Executed/Current	Starting Date / Time	Elapsed Time	CPU Time
0	ABC	OPERATOR	WOLOGON OFFICE2	12/28 10:10	10:11	0:05:43
172	SRB		WOLOGON WP	12/28 10:12	10:12	0:06:23
252	JSS		WOLOGON OFFICE2	12/28 9:12	9:13	0:02:13
253	RLZ		WOLOGON OFFICE2	12/28 8:15	8:15	0:04:42
254	LAJ		WOLOGON OFFICE2	12/28 10:30	10:30	0:04:12

Position cursor to indicate task and press PFkey to perform action:

(7) Paging & I/O
(8) Program status
(6) Non-interactive tasks
(11) Change status
(12) Cancel program
(13) Logon/Logoff control

Figure 6-5. Sample Control Interactive Tasks (Status and Time) Screen

The Control Interactive Tasks screen displays the following information:

WS -- The workstation number assigned to this task.

User -- The ID of the user logged on at this workstation.

Status -- The status of user activity at this workstation. The status can be OPERATOR, IDLE, DEBUG, HELP PROCESSOR, or IN CANCEL.

Program Executed/Current -- The name of the program or procedure currently being run.

Starting Date/Time -- The date and time that the program or procedure was started.

Elapsed Time -- The time that has elapsed since you started the program or procedure.

CPU Time -- The CPU time used in executing a program or procedure.

Control Interactive Tasks Screen Functions

The Control Interactive Tasks screen contains the following functions:

PF2 - PF5 -- Scrolls through the complete list of interactive tasks, nine at a time. PF2 displays the first screen, PF3 the last screen, PF4 the screen previous to the current one, and PF5 the screen after the current one.

PF6 (Non-interactive tasks) -- Displays the Control Non-Interactive Tasks screen on your workstation. This function allows you to examine and modify the noninteractive (background) tasks on your local system. All operations are available to you, just as they are when you enter this menu directly from the VS Operator's Console. For information on controlling noninteractive tasks, refer to the *VS System Operator's Guide*.

PF7 (Paging & I/O) -- Displays the Paging & I/O menu. Statistical information on paging and I/O for each workstation is displayed. You can use this information to access the total resource requirements of a program and to determine how efficiently the program uses memory. The Paging & I/O menu can also be used to troubleshoot system page pool errors. Using Paging & I/O information, you can determine which tasks are using the page pool in question.

The Paging & I/O menu also totals and displays the number of input/output operations that have taken place between the system and peripheral devices. The information displayed for each task is as follows:

WS I/O -- The number of workstation input/output operations

Disk I/O -- The number of disk input/output operations

Tape I/O -- The number of tape input/output operations

Print I/O -- The number of print input/output operations

Other I/O -- The number of other input/output operations (including telecommunications)

Page-Ins System -- The total page-ins used by the system for this task

Page-Ins Program -- The total number of page-ins used by the program

Page-Outs System -- The total number of page-outs used by the system

Page-Outs Program -- The total number of page-outs used by the program

To return to the Control Interactive Tasks screen, press PF7.

PF8 (Program status) -- Provides file information for any program or procedure being run from a workstation. To access this screen, position the cursor next to the workstation's entry and press PF8. The program or procedure name, library, file names, and the number of open files appear on the screen. The Program Status screen displays the following information for each file:

Unit -- The type (disk, workstation, etc.) on which the file resides.

Address -- The unit number of the device. This represents the last or current disk accessed for volume sets.

Mode -- The mode used by the program or procedure to open the file (e.g., INPUT, OUTPUT, I/O, EXTEND, SHARED, DMS/TX).

XIO Count -- The current total of input/output transfers.

File -- The name of the file.

Library -- The name of the volume in which the file resides.

Volume -- The volume name in which the library resides.

Extents -- The number of extents assigned to the file.

The data presented on the Program Status screen cannot be modified. It is presented for informational purposes only. You can exit this screen and return to the Control Interactive Tasks screen by pressing PF1 (Return to task control display).

PF11 (Change Status) -- Change the status of an interactive task. Position the cursor next to the entry that you want to change and press PF11.

You can interrupt interactive programs and procedures to enter the Help mode. This causes the Modified Command Processor to be displayed at the originator's workstation. Any program compiled with the SYMB=YES, the debugger flag, can be interrupted, allowing the user access to the debugger.

The Change Status screen also allows you to enable and disable temporary and permanent operator privileges for any workstation. Assignment of operator privileges permits a workstation to have dual mode privileges; this allows access from that workstation to both the VS Command Processor menu and the VS Operator's Console menu.

To perform any of these operations, press the appropriate PF key. The keys and their associated actions are as follows:

(2) (Cause task to enter HELP processor)
(3) (Allow task interactive DEBUG access)
(5) (ENABLE, or DISABLE temporary operator privileges)
(6) (ENABLE, or DISABLE permanent operator privileges)

Press PF1 to exit the Change Status screen, and return to the Control Interactive Tasks screen.

PF12 (Cancel Program) -- Cancel an interactive program. Position the cursor next to the workstation entry from which the program is running and press PF12. The Cancel Program screen appears.

The originating user's logon, workstation number, program name, and program status (e.g., IDLE, EXECUTING) are displayed across the top of the screen. Pressing ENTER initiates the cancel operation. An additional option is presented to allow programmed interception of the cancel operation. This option enables you to override the cancel operation. Enter YES or NO in this field. The default is NO.

When you press ENTER, the system returns to the Control Interactive Tasks screen. To return to the Control Interactive Tasks screen without canceling the program, press PF1.

PF13 (Logon/Logoff control) -- Control the logon and logoff capabilities of the workstations on your system. This function provides a wide range of control capabilities. You can log an individual user off immediately, set a workstation to log off the user as soon as a currently running procedure or program is completed, or inhibit future logons as soon as the current user logs off. You also have the option to automatically log off inactive workstations.

To initiate logon/logoff control, position the cursor next to a workstation entry on the Control Interactive Tasks screen and press PF13. When you are controlling an individual workstation, place the cursor next to that workstation's entry. When you are controlling all workstations, position the cursor next to any entry. In either case, pressing PF13 causes the Control LOGON/LOGOFF screen to appear at your workstation.

When you are controlling individual workstations, the Control LOGON/LOGOFF screen contains four PF key control functions:

(3) INHIBIT logons (without affecting user)
(5) LOGOFF user at program (or procedure) COMPLETION
(6) LOGOFF user IMMEDIATELY
(7) ENABLE automatic LOGOFF

Additionally, PF1 can be used to return to the Control Interactive Tasks screen without affecting any workstation.

Press PF3 to inhibit logons without affecting any users who are currently logged on to a workstation. When a user logs off, that workstation is then inhibited for any future logon. This function can also be performed with the Control Workstations function (PF13) on the Operator's Console, as described later in this chapter. To allow logon for a workstation after you have inhibited logon, use the Control Workstations function (PF13). The two logoff functions, PF5 and PF6, affect the current user only.

The PF7 key functions as an enable/disable switch for automatic logoff. Once auto logoff is enabled, the screen display for PF7 reads "DISABLE automatic LOGOFF." When the automatic logoff function is enabled, the system monitors the length of time each workstation is inactive. When a time limit, as specified through the Set System Parameters screen of the Operator's Console, is reached, the system automatically logs a workstation off. The automatic logoff function can be enabled or disabled for individual workstations. Automatic logoff is disabled by default for a workstation.

Caution: *The system forces the cancellation and logoff of a data processing task running on a workstation selected for automatic logoff if it does not receive an unsolicited interrupt (e.g., PF key, HELP key, or ENTER key) during the specified time interval. Automatic logoff is not in effect when a workstation is in word processing mode. In a situation where a line has been disconnected, all workstations except the 2246R or 4220 series workstations will be automatically logged off.*

Automatic logoff is in effect for all data processing tasks on the selected workstations. For example, a program that continuously displays the time of day on a selected workstation will be canceled and the workstation logged off if the system does not detect a user response during the specified time interval.

To initiate the automatic logoff function, you must first establish the time limit, using the Set System Parameters screen. To access this screen, press PF4 from the System Options screen of the Operator's Console.

To control logon and logoff operations for all workstations, press PF10 from the Control Logon/Logoff screen. Your current screen changes, displaying PF key functions that enable you to allow and inhibit logons, disconnect workstations, and log off users immediately or at program or procedure completion. These functions are

(2) ALLOW logons
(3) INHIBIT logons (without affecting user)
(4) INHIBIT logons and DISCONNECT workstations
(5) INHIBIT logons and LOGOFF users at program (or procedure) completion
(6) INHIBIT logons and LOGOFF users IMMEDIATELY

These control functions are also available through the Control Workstations function on the VS Operator's Console. Just as you must use the Control Workstations function to enable any single, logon-inhibited workstation, you must also use it to enable all workstations once they have been inhibited. The Control Workstations function is described later in this chapter.

CONTROLLING COMMUNICATIONS

The control functions described in this section are listed on the Control Communications screen (Figure 6-6). From this screen, you can access information about all telecommunications controllers configured for the system, including all remote devices connected by telecommunications lines. To access the Control Communications menu, press PF12 (Telecommunications) from the VS Operator's Console menu.

Note: *Network users can access this information with the Manage Communications function on the VS Command Processor menu. However, there are no control options.*

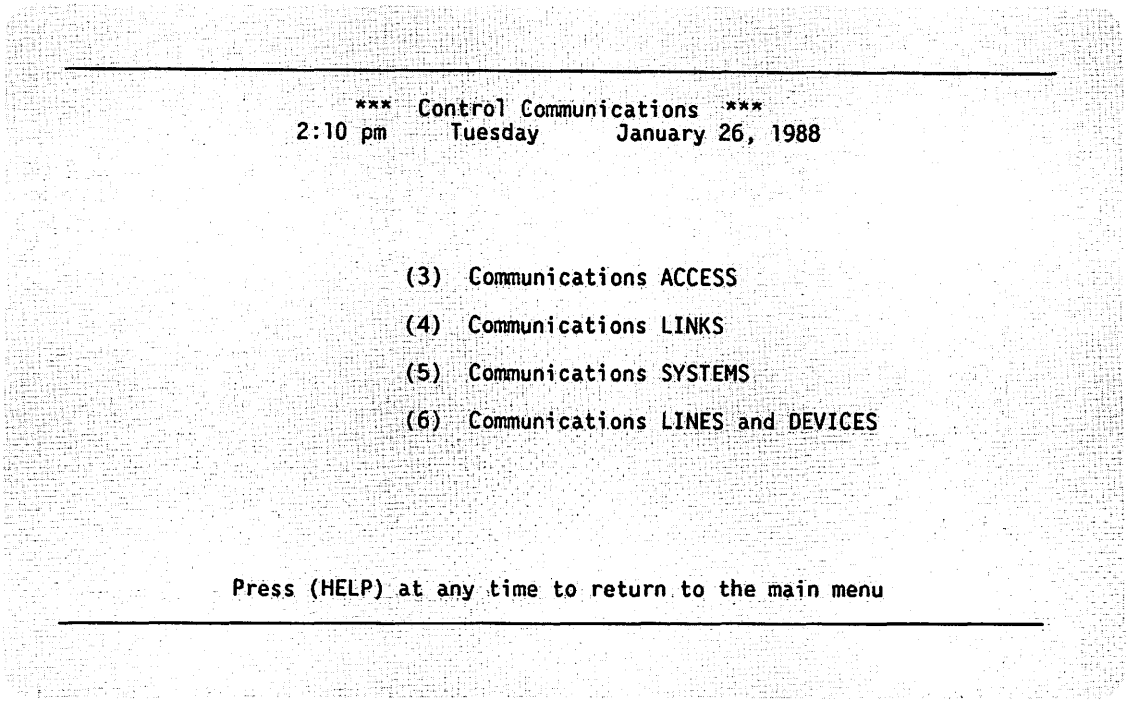

Figure 6-6. Control Communications Menu

Communications Access

To control communications between your system and all other systems, press PF3 (Communications Access). The Control Communications Access screen (Figure 6-7) gives you the option to allow communications, inhibit any new sessions, or immediately stop all sessions (file transfer and logon).

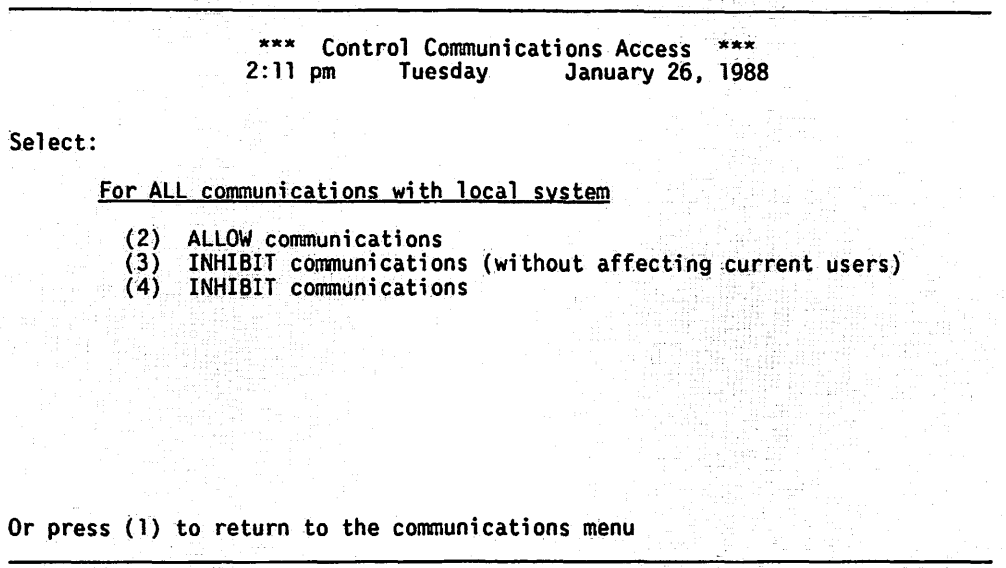

Figure 6-7. Control Communications Access Menu

From the Control Communications Access menu, you can perform the following functions:

PF2 (ALLOW communications) -- Allows all properly configured remote systems access to your VS through either the VS Terminal Emulation, the Virtual Terminal Interface, or the File Transfer service.

PF3 (INHIBIT communications (without affecting current users)) -- Inhibits any new sessions with your VS. Pressing this key does not affect current users (users who have established active sessions with your system); they can complete their sessions.

PF4 (INHIBIT communications immediately) -- Causes your system to inhibit any new sessions and stop all current sessions. Sessions that your system interrupts return to their original status. For example, pressing PF4 during a File Transfer session returns the document or file being transferred to the transfer queue of the sending system; it is transferred the next time a session is established.

After you press the appropriate PF key, the system prompts you to confirm your selection. Press ENTER to confirm your choice.

Communications Links

To control communications with all systems on a specific link or DLP, press PF4 (Communications Links) on the Control Communications menu. The screen displays a list of links on your system, and the names of the systems on each link. Figure 6-8 illustrates a sample Control Communications Links screen. Press TAB to position the cursor next to the name of the link you want to control and press PF6 (Control Link).

```
                *** Control Communications Links ***
              2:12 pm     Tuesday     January 26, 1988

* 29 links on system

  Link              System on link          Status
  {non-adjacent}    ITRC                    No sessions active
                    TERMINAL                No sessions active
  DIALUPNETVS       HERVE                   No sessions active
  TESTSNALINK       OA32SYS                 No sessions active
                    SYS14                   No sessions active
  068ALINK          VS1                     No sessions active
  WANGBANDLINK2     VS1K                    No sessions active
                    VS2                     No sessions active

                  Position cursor to indicate link and select:

(1) Menu
                (5) Next                  (6) Control link
(3) Last
```

Figure 6-8. Sample Control Communications Links Screen

When you press PF6 (Control link), the screen displays the same options as those described in the previous section, and the options are accessed by the same PF keys. The keys and the options accessed are as follows:

(2) ALLOW communications
(3) INHIBIT communications (without affecting current users)
(4) INHIBIT communications

However, pressing any one of these PF keys affects communications only on the link you select.

Communications Systems

To access Communications Systems, press PF5 on the Control Communications menu. This option lets you control and monitor communications services between your VS and a specific remote system. The Control Communications Systems screen (Figure 6-9) lists each connected system. One line is used for each service available for that system. The Link column lists the names of the transports, as configured in the WSNEDIT utility. If the service is inhibited, the word "inhibited" appears. If it is not, the number of logons and transfers in progress is shown. A status of "Assistance Required" is shown if the operator must dial a phone number to connect the remote system.

```
                    *** Control Communications Systems ***
                    2:15 pm     Tuesday     January 26, 1988

System          Link              Service          Status
ATLAS           WANGBANDLINK1     Inbound Logons   3 users logged on
                                  File-Transfers   No transfers in progress
COBBER          WANGBANDLINK1     Inbound Logons   2 users logged on
                                  File-Transfers   1 transfer in progress
DIGGER          WANGBANDLINK1     Inbound Logons   No users logged on
                                  File-Transfers   No transfers in progress
DMFCNTRL        WANGBANDLINK1     Inbound Logons   No users logged on
                                  File-Transfers   No transfers in progress
DUNE            WANGBANDLINK1     Inbound Logons   2 users logged on
                                  File-Transfers   1 transfer in progress

                Position cursor to indicate system and select:

(1) Menu
                (5) Next    (6) Control service at system
(3) Last                                          (11) Session information
```

Figure 6-9. Sample Control Communications Systems Screen

The communications services that your VS supports include document and file transfers and inbound logons (logons to your VS).

Under the first column heading, System, this screen lists the name of each system. The second column, labeled Link, lists the name of the link through which you can access the particular system. The third column, Service, lists the service associated with each system. The last column indicates the status of each system's services. For an inhibited service, the word "Inhibited" appears in the Status column; otherwise, the screen shows the number of inbound logons (and the number of transfers in progress).

Controlling Communications Services and Sessions

From the Control Communications Systems screen, you can control all sessions that are using a specific service available to the system that you choose. You make your choice by pressing PF6 (Control service at system), or you can select the remote system and choose to control its individual sessions (that is, specific transfers and logons) by pressing PF11 (Session information).

By pressing PF6 (Control service at system), you can inhibit or enable a specific service for the system you select. This key can call up two different screens, one for each type of service. The position of the cursor at the time this key is pressed determines the choice of screen. For example, to inhibit all File Transfer sessions from a remote system, move the cursor to the File Transfer selection for that system and press PF6. The system displays the Control File Transfer screen, lists the name of the remote system, and offers two options: PF3 (Inhibit Transfers without affecting active transfers), and PF6 (Inhibit Transfers, Cancel active transfers and HOLD Entries).

Press PF11 (Session information) if you want a list of all active sessions that involve the remote system you select. Figure 6-10 shows a sample Control Sessions screen for a remote system.

```
                    *** Control Sessions ***
2:20 pm      Tuesday       January 26, 1988

                        System ALTAS

File Transfer:
      Transmitting INVENTRY in INVENLIB on SYSTEM for Remote User MLL
      Retrieving MAIL in MAILLIB on SYSTEM for Local user ROD

Inbound Logons:
      Workstation 254, User LAJ (Larry Jones)
      Workstation 252, User JSS (John Smith)


              Position cursor to indicate session and select:

(1) Return
                              (6) Control session
```

Figure 6-10. Sample Control Sessions Screen

To control an Inbound Logon session, position the cursor next to the name of that session and press PF6 (Control Session). You can then disconnect the remote workstation by pressing PF4, log off the remote user immediately by pressing PF6, or log off the remote user at program completion by pressing PF5.

When the cursor is next to a File Transfer session and you press PF6 (Control Session), you can cancel the current transfer and requeue it with a status of "hold" by pressing PF6 again.

Communications Lines and Devices

To control communications lines and devices, press PF6 on the Control Communications menu. Figure 6-11 illustrates a sample Control Communications Lines screen. The screen displays the DLP names, type, link name, number of devices configured to each DLP, the transport protocol loaded to each DLP, and the current status of each DLP.

```
                    *** Control Communications Lines ***
                    2:21 pm     Tuesday     January 26, 1988

15 lines in system

DLP Name    Type      Link Name    # Devices    Protocol    Status
144A        23V97W                     5
144B        23V97W                     1
144C        23V97W                     2
176I        23V97W                     4                   Reserved
176J        23V97W                     4
176K        23V97W                     4
176P        23V97W                     2

                    Position cursor to indicate line and select:

(1) Menu                    (6) Manage devices on the line
                            (7) Activate/Change Protocol
(3) Last    (5) Next        (8) Deactivate
```

Figure 6-11. Sample Control Communications Lines Screen

The Control Communications Lines screen displays the following information:

DLP Name -- The DLP name is a 4-character data item. The first three numeric characters identify the lowest device number on the device adaptor (DA), input/output processor (IOP), or I/O controller (IOC) line. The fourth character is a letter that identifies the port. All lines on the same IOP or DA have the same first three bytes.

Type -- Describes the DA, IOP, or IOC by model number.

Link Name -- The name of the link (up to eight characters) as specified in GENEDIT.

 # Devices -- Shows the number of virtual circuits configured to the line.

Protocol -- Identifies the type of protocol used on the line. This file can be modified by VS300 systems only.

Status -- Indicates whether the line is being used (reserved) or not (blank).

The Control Communications Lines screen contains the following functions:

PF2 - PF5 -- Scrolls through list of available lines. PF2 displays the first screen, PF3 the last screen, PF4 the screen previous to the current one, and PF5 the screen after the current one.

(6) Manage devices on the line -- Displays the status of a specific DLP. If the DLP is not running, either a blank space occupies the Status field, or the DLP type is displayed (TCB1, TCB3, or CIU). If the DLP is active, its status appears as "Reserved and In Use." The control path for each DLP uses the lowest device number. Your VS should label it "Reserved."

(7) Activate/Change Protocol -- Enables you to change the protocol currently being used by the specific DLP. Enter the name of the protocol that you want to load to the DLP. To display the list of available protocols, press PF2.

(8) Deactivate -- Enables you to deactivate a DLP to make it unavailable for further use until it is reactivated.

When you press PF6 (Manage devices on the line), a screen similar to one shown in Figure 6-12 appears. The information on the Control Communications Devices screen is listed in order by unit number (device address). The following information is provided for all telecommunications controller devices:

- Unit (device address)
- Type (device model number)
- Line (line name)
- Routing address
- Status

If the unit currently has no device associated with it, the Type column lists it as available. If the device is a remote workstation, the Status column contains the associated task's user ID. The valid devices are listed in the GENEDIT utility.

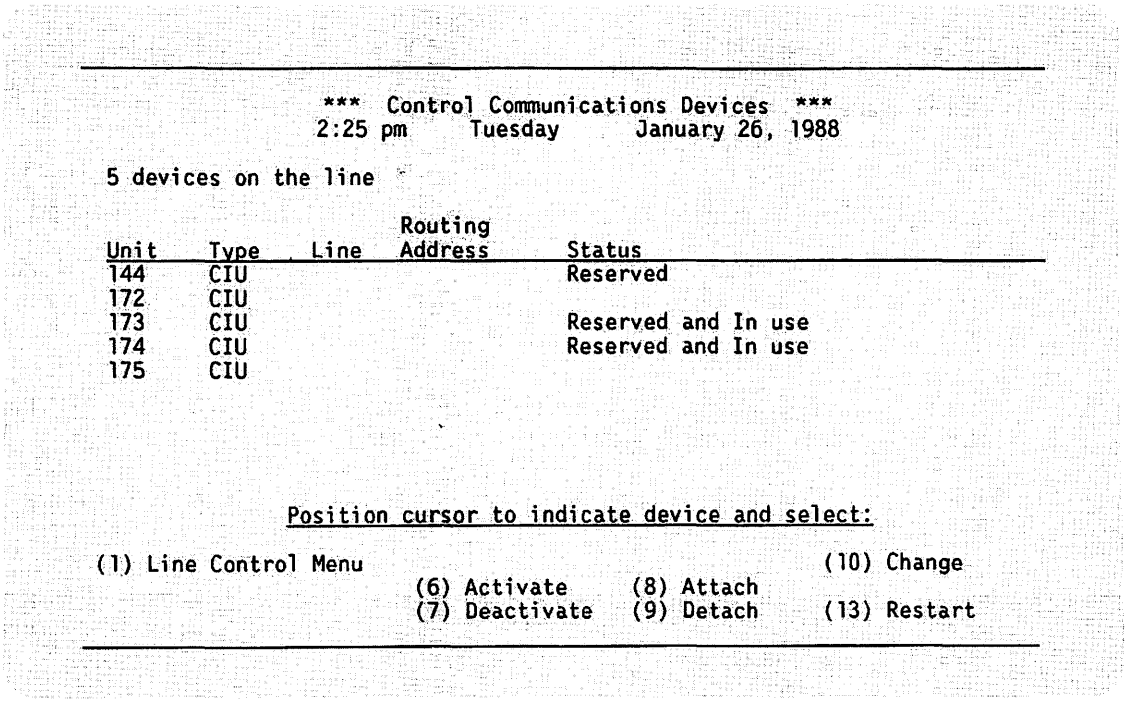

Figure 6-12. Sample Control Communications Devices Screen

The screen shows the status of each of the devices (virtual circuits) configured to the DLP you selected on the Control Communications Lines screen. The screen displays the following information:

Unit -- Unit numbers are specified in the configuration file.

Type -- If the unit has a device associated with it, the Type column displays the device model number. If the unit currently has no device associated with it, the Type column lists it as available.

Line -- The user-specified line name. The name can contain up to eight alphanumeric characters.

Routing Address -- Indicates a number from 0 to 31. The number indicates the position of the device on the line dropped from the modem.

Status -- Indicates the device as Activated, Detached, Logged on, Reserved, or Reserved and In Use, depending on the actual status of the device.

You can perform the following functions to change the state of the devices:

(6) Activate -- Allows you to activate a device

(7) Deactivate -- Allows you to deactivate a device

(8) Attach -- Allows you to attach a device

(9) Detach -- Allows you to detach a device

(10) Change -- Allows you to change the status of a device

(13) Restart -- Allows you to restart a device

CONTROLLING WORKSTATIONS

The Control Workstations screen (Figure 6-13) provides information about all local workstations that are configured on your local system and all remote workstations that are currently connected. This information is listed in order by unit number (device address). To access the Control Workstations screen, press PF13 (WORKSTATIONs) on the VS Operator's Console.

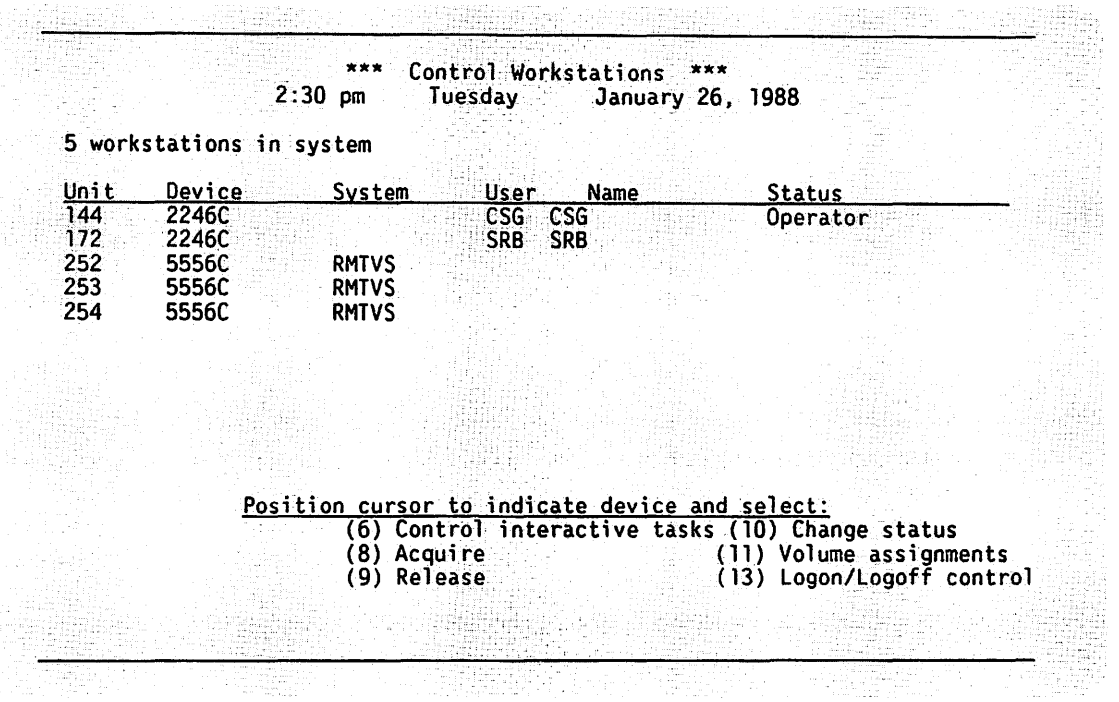

Figure 6-13. Sample Control Workstations Screen

The Control Workstations screen displays the following information:

Unit -- The workstation device numbers for inbound logons (logons to your system).

Device -- The workstation model number.

System -- The system name appears only if the workstation is a remote workstation. It specifies the name of the remote system whose user is logged on (inbound) to your VS.

User -- The user ID appears if the user is logged on.

Name -- The user name appears if the user is logged on.

Status -- The status appears for any workstation that is not READY. "Operator" is displayed in the status column if the workstation is an operator's console. A status of "Disconnected" indicates that a local workstation is physically disconnected from the network or powered off.

From the Control Workstations screen, you can perform the following functions:

PF6 (Control interactive tasks) -- Displays the Control Interactive Tasks screen.

PF8 (Acquire) -- Logically reconnects a released workstation to the VS. Position the cursor next to the name of the released workstation (its status column displays "Released") and press PF8. Press ENTER to verify your selection.

PF9 (Release) -- Logically disconnects a workstation from the VS. Position the cursor next to the name of the appropriate workstation and press PF9. Press ENTER to verify your selection. "Released" is then displayed in the Status column for this workstation. This permits you to run standalone tasks on the workstation, such as diagnostics.

PF10 (Change Status) -- Changes the status of the workstation. Position the cursor to the left of the name of the selected workstation and press PF10 to access the Change Status screen. From the Change Status screen, you can perform the following operations:

- Cause a task to enter the HELP Processor (PF2)
- Allow a task interactive DEBUG access (PF3)
- Enable temporary operator privileges (PF5)
- Enable permanent operator privileges (PF6)

PF11 (Volume Assignments) -- Displays the Volume Assignments screen. The Volume Assignments function is a control mechanism for solving special problems with paging files.

The Volume Assignments screen provides a control mechanism that allows you to override the system paging volume selection algorithm. It also allows you to assign an interactive task to a volume to solve special problems affecting page file placement. To modify the volume assignment, position the cursor next to an entry and press PF10. The Paging Assigned column is then highlighted; enter the volume name and press ENTER. The volume assignment takes effect the next time a user logs on to that workstation. The system retains the paging volume assignments across IPLs.

This control mechanism enables you to compensate for situations where the majority of I/O activity may not be caused by paging. If, for example, a volume contains an extremely active data file, you may want to offset that activity by disabling paging on that volume or by placing a number of paging files on another volume. You can place paging files on a particular volume by assigning certain workstations to the volume. Once the I/O activity is balanced, the default algorithm can take over to keep the activity even.

Note: *Use the volume assignment control mechanism for special situations only. If applied indiscriminately, it may degrade rather than improve performance.*

For additional information on the allocation and placement of paging files, refer to the *VS Systems Utilities Reference*.

PF13 (Logon/Logoff control) -- Initiates logon and logoff control. Position the cursor to the left of a workstation entry and press PF13 to access the Logon/Logoff Control screen. From this screen you can control a single workstation, or you can control all workstations. For information on the Logon/Logoff Control screen, refer to the section in this chapter entitled, *Controlling Interactive Processing Tasks*.

CHAPTER 7
USING THE WANG BAND MONITOR

OVERVIEW

This chapter describes the Wang Band Monitor. The Wang Band Monitor is the VS software tool that allows you to display status information from the Cable Interface Units (CIUs) that are attached to each system in your network. A CIU (internal or external) is the hardware device that connects a VS system to the WangNet Wang Band cable. The Wang Band Monitor polls or requests data from each CIU to provide you with the following status information:

- A listing of all systems on the Wang Band, as defined on your local system, whether or not a system was able to respond to a Wang Band Monitor poll, and the number of virtual circuits that are currently active on each successfully polled system

- The circuit status of a selected system on the Wang Band, including the number of virtual circuits that are supported by the CIU type (internal or external), and the current state of each virtual circuit

- The unit status of a selected system on the Wang Band, including general network traffic information and error counts

ACCESSING THE WANG BAND MONITOR

The Wang Band Monitor capabilities are contained in the program LWNMON, which can be accessed through the Run Program or Procedure function (PF1) from the Wang VS Command Processor screen.

To access the Wang Band Monitor, perform the following steps:

1. Log on to the VS. The VS Command Processor screen appears.

2. Press PF1, Run Program or Procedure. The Run screen appears.

3. Type LWNMON as the procedure name, and press ENTER.

When you specify the LWNMON program from the Run Program or Procedure screen, the first Wang Band Monitor screen appears. This screen requests the name of the Wang Band link that you want to monitor. Figure 7-1 shows an example of a Wang Band Link To Monitor screen with an entry filled in.

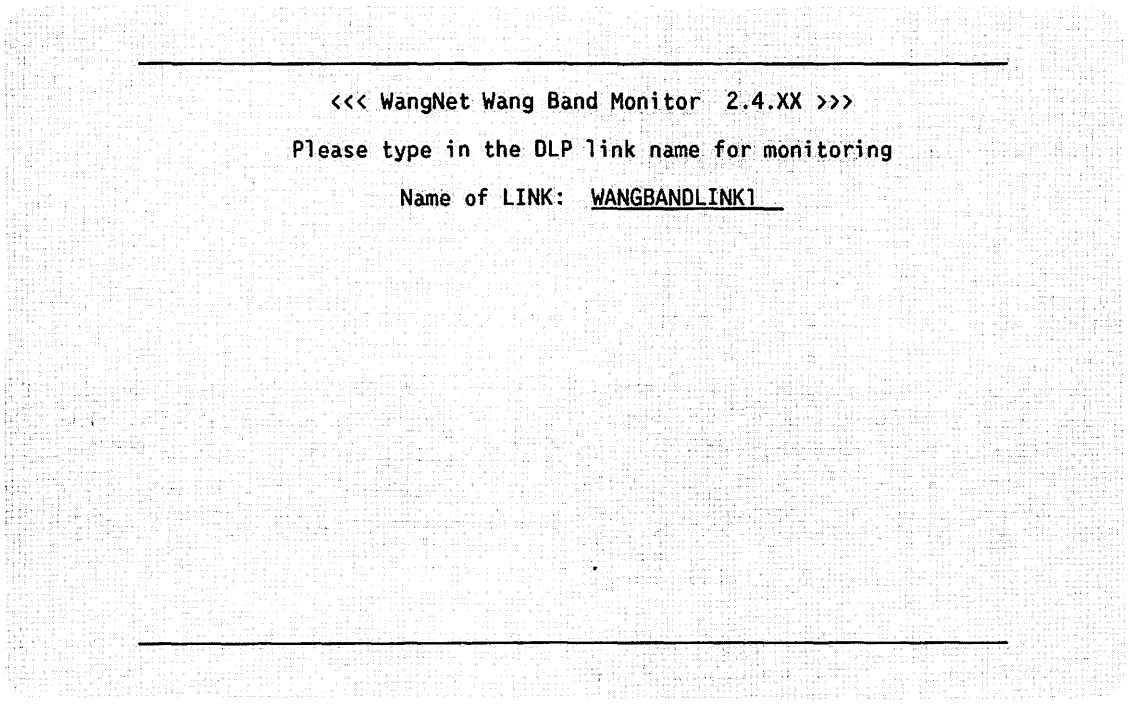

Figure 7-1. Wang Band Link To Monitor Screen

When you display the Wang Band Link To Monitor screen, the default Wang Band transport name appears. The default is the name of the first Wang Band transport configured to your local system. The transports are those that were previously configured through the WSNEDIT Manage Transports function.

The next Wang Band Monitor screen lists the systems on the network that are connected by Wang Band to your local system. Figure 7-2 shows an example of such a screen.

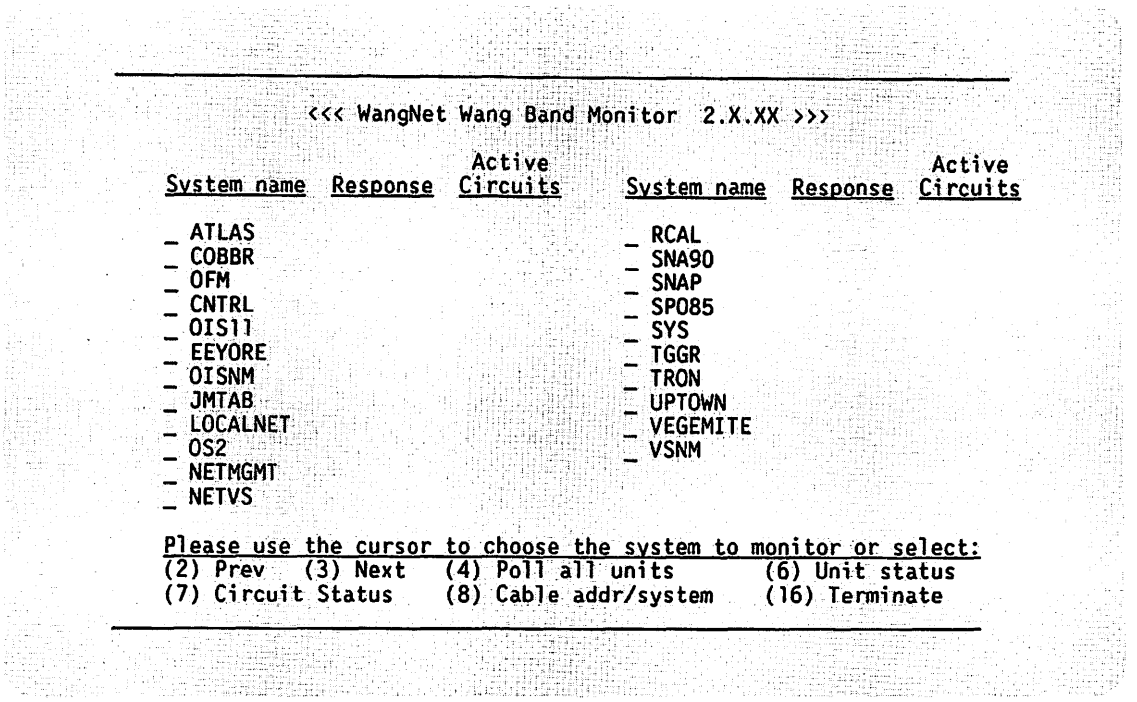

Figure 7-2. Wang Band Monitor System Screen

Wang Band Monitor System Screen Functions

Table 7-1 describes the functions on the Wang Band Monitor System Screen.

Table 7-1. Wang Band Monitor System Screen Functions

When You Press	You Can
PF2 (First) PF3 (Last)	Scroll through the list of system names when the list consists of more than one screen.

(continued)

Table 7-1. Wang Band Monitor System Screen Functions (continued)

When You Press	You Can
PF4 (Poll all units)	Instruct the Wang Band Monitor to sequentially poll the CIUs that are attached to systems in the list. When you press PF4, the Wang Band Monitor begins to poll all the Cable Interface Units (CIUs) in sequence and displays the results of those polling attempts on the screen (see Figure 7-3). The arrow points to the system currently being polled. To stop polling, press PF16 (Terminate).
PF6 (Unit status)	Instruct the Wang Band Monitor to display the CIU traffic statistics and error counts associated with the system that you selected from the list.
PF7 (Circuit Status)	Instruct the Wang Band Monitor to display the virtual circuit status for the system that you selected from the system list. The Circuit Status screen displays the total number of virtual circuits that are supported for the type of CIU being monitored, the state of each virtual circuit, and the remote system name (or cable address) currently using that circuit.
PF8 (Cable addr/system)	Display the cable addresses rather than the system names that appear on the Wang Band Monitor screens. When you press PF8, all system names appearing on your current screen change to the corresponding WangNet cable addresses. To redisplay the system names, hold down the Shift key and press PF8.
PF16 (Terminate)	Exit from the Wang Band Monitor program and return to the Wang VS Command Processor screen.

Polling All Units

When you press PF4 from the Wang Band Monitor System screen, the Wang Band Monitor begins to sequentially poll the CIUs. This function displays the current on- or off-line status of each CIU, and the number of virtual circuits currently established to remote systems. During the monitoring process, an arrow appears to the right of a system name to indicate that the CIU (used by that system) is currently being polled.

If a CIU is on-line, "YES" appears in the Response field to the right of the system name. An on-line CIU also displays the number of active virtual circuits to a remote system that are currently established. If a CIU does not respond to a Wang Band Monitor poll, the poller waits 3 seconds before declaring the CIU off-line. If a CIU is off-line, "NO" appears in the Response field, and the Active Circuits field remains blank.

When all CIUs have been polled, the Wang Band Monitor restarts the polling process to display the latest results, starting with the first system named in the list.

To stop the Wang Band Monitor Poll All Units function, press PF16. This terminates the program and returns you to the Wang VS Command Processor Screen.

Figure 7-3 shows a sample Poll All Units screen.

```
                <<< WangNet Wang Band Monitor  2.X.XX >>>

                             Active                                  Active
System name   Response   Circuits      System name   Response   Circuits

_ ATLAS          YES          1         _ RCAL           NO
_ COBBR          NO                     _ SNA90          YES         4
_ OFM            YES          0         _ SNAP           YES         0
_ CNTRL          NO                     _ SP085          NO
_ OIS11          NO                     _ SYS            YES         1
_ EEYORE         YES          0         _ TGGR         ->
_ OISNM          YES          0         _ TRON
_ JMTAB          NO                     _ UPTOWN
_ LOCALNET       NO                     _ VEGEMITE
_ OS2            YES          0         _ VSNM
_ NETMGMT        NO
_ NETVS          NO

Please use the cursor to choose the system to monitor or select:
(2) Prev   (3) Next   (4) Poll all units       (6) Unit status
(7) Circuit Status    (8) Cable addr/system    (16) Terminate
```

Figure 7-3. Wang Band Monitor Polling All Units Screen

The functions displayed at the bottom of this screen are described in the sections that follow.

Circuit Status

When you select a system from the Wang Band Monitor System screen and press PF7 (Circuit Status), the screen displays the status of the CIU's virtual circuits. If the system you select is using an internal CIU (VS 300 and VS 7000 Series systems), your Circuit Status screen displays the state of the 63 virtual circuits. If the system is using an external CIU, the screen displays the state of 24 virtual circuits.

The Wang Band Monitor Circuit Status screen always shows the maximum number of virtual circuits (63), regardless of the CIU type.

The state of each virtual circuit can be

Up -- The virtual circuit is active.

Down -- The virtual circuit is inactive.

Not Available -- The virtual circuit is not available, or the CIU is an external CIU.

Under the heading "System," the Wang Band Monitor Circuit Status screen also displays the name of the remote system using each virtual circuit.

Figure 7-4 shows an example of a Wang Band Monitor Circuit Status screen that is using an external CIU.

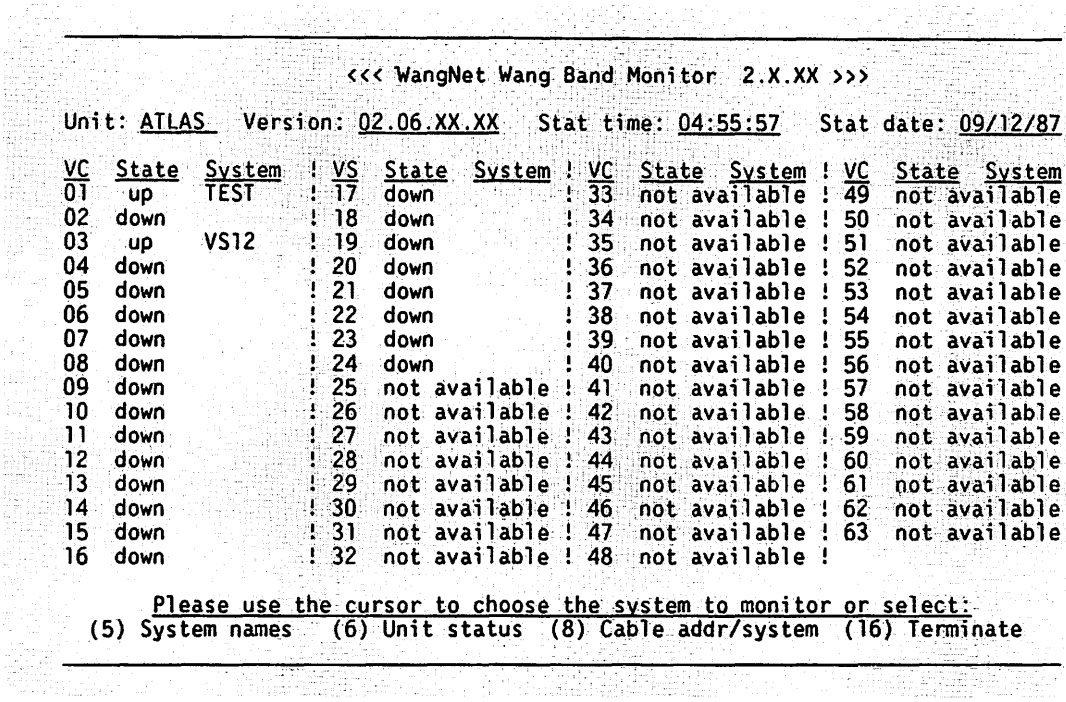

Figure 7-4. Wang Band Monitor Circuit Status Screen

Table 7-2 describes the functions on the Wang Band Monitor Circuit Status screen.

Table 7-2. Wang Band Monitor Circuit Status Screen Functions

When You Press	You Can
PF5 (System Names)	Return to the Wang Band Monitor System Screen.
PF6 (Unit status)	Instruct the Wang Band Monitor to display CIU traffic statistics and error counts that are associated with the system that you selected from the list.
PF8 (Cable addr/system)	Change the remote system names to their corresponding cable addresses. If you hold down the Shift key and press PF8, the system names reappear.
PF16 (Terminate)	Exit from the Wang Band Monitor program and return to the Wang VS Command Processor screen.

Unit Status

When you select a system from the Wang Band Monitor System screen and press PF6, or if you press PF6 from the Circuit Status screen, the Unit Status screen appears. Figure 7-5 shows an example of such a screen. This screen displays the decimal and hexadecimal totals of network traffic statistics and error counts from the CIU.

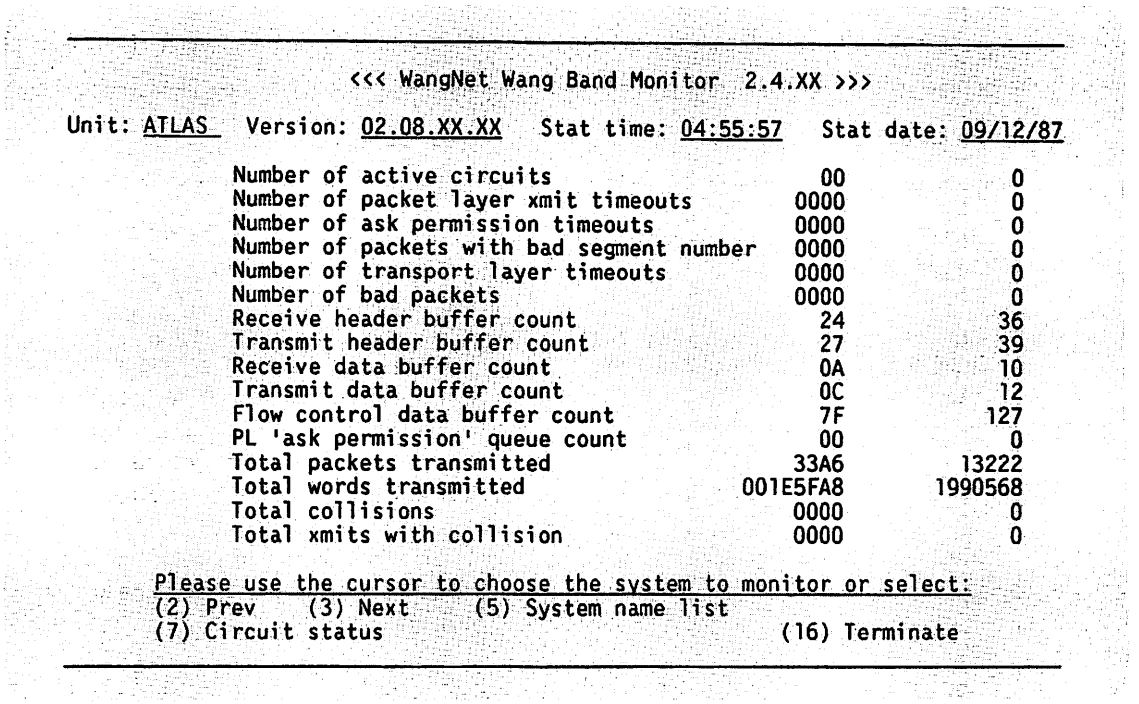

Figure 7-5. Wang Band Monitor Unit Status Screen

Table 7-3 contains a complete listing of the unit status messages and their meanings.

Table 7-3. Wang Band Monitor Unit Status Messages

Message	Meaning
Number of active circuits	Total number of inbound and outbound sessions currently active.
Number of packet layer xmit timeouts	Number of times a packet had to be retransmitted because no ack signal was received within the timeout period.
Number of ask permission timeouts	Number of times a flow control packet had to be retransmitted because no response was received within the timeout period.

(continued)

Table 7-3. Wang Band Monitor Unit Status Messages (continued)

Message	Meaning
Number of packets with bad segment number	Number of times a packet was discarded because of an invalid control field.
Number of transport layer timeouts	Number of times a circuit was cleared because the higher layer (VS or OIS host application) did not read a pending message before the end of the timeout period.
Number of bad packets	Number of times a packet was discarded because it was received garbled.
Receive header buffer count	Number of buffers available to receive control packets. A lower number indicates a high amount of traffic or delay in this unit.
Transmit header buffer count	Number of buffers available to transmit control packets.
Receive data buffer count	Number of buffers available to receive user data packets.
Transmit data buffer count	Number of buffers available to transmit user data packets.
Flow control data buffer count	Maximum allowable number of buffers to be allocated to messages in flight. This value is the upper limit on the 'ask permission' queue count.
PL 'ask-permission' queue count	Outstanding number of requests to transmit long user data packets.
Total packets transmitted	Number of control and user data packets transmitted.
Total packets received	Number of control and user data packets received.

(continued)

Table 7-3. Wang Band Monitor Unit Status Messages (continued)

Message	Meaning
Total words transmitted	Number of 16-bit words in all packets transmitted.
Total collisions	Number of times a packet had to be retransmitted because of collision.
Total xmits with collisions	The number of packets that were involved in at least one collision.
Total words received	Number of 16-bit words in all received packets.
Error record high and low bits	OR'ed error status bits for all receptions and transmissions. A bit set indicates that the corresponding error occurred at least once. Bit values are
8000	Reserved.
4000	A packet was received that was larger than the agreed upon maximum packet size.
2000	Reserved.
1000	Memory did not respond fast enough during a reception.
0800	The packet received did not have a closing flag or was not a multiple of 16 bits.
0400	Receive memory address overflowed X'FFFF'.
0200	CRC error detected.
0100	Abort character received.
0080	Data Set Ready signal went off.
0040	Data Terminal Ready signal went off.

(continued)

Table 7-3. **Wang Band Monitor Unit Status Messages** (continued)

Message	Meaning
0020	Reserved.
0010	Maximum number of collision retries was exceeded on xmit.
0008	Reserved.
0004	Reserved.
0002	A transmit was aborted, either because of slow memory or parity error.
0001	Reserved.
Receive abort count	An abort character detected in an incoming packet.
CRC error count	CRC error detected on received packet.
Address overrun count	Attempt to store an incoming packet past memory address X'FFFF'.
Framing error count	A packet was received that did not have a closing flag or did not contain a multiple of 16 bits.
Memory overrun count	Memory did not respond fast enough during a receive operation.
Data overrun (frame size exceeded) count	Frame size exceeded during a receive operation

CHAPTER 8
USING THE WSN CONFIGURATION REPORTER

OVERVIEW

The WSN Configuration Reporter is a VS tool that allows you to generate reports from the information contained in your network's current configuration file. When you create and print these reports, you can easily view the network configuration information without accessing the WSNEDIT utility. You can refer to the reports when you are planning for network expansion or when you want to make adjustments to your current configuration for more efficient network operation.

The WSN Configuration Reporter allows you to generate the following reports:

Network Routing Summary -- Lists areas and systems to which paths have been defined. The report includes next hop systems, path costs, transports, and the base cost associated with each transport.

Service Summary -- Lists all systems and the services defined for each system. The report includes CNS, File Transfer (CNS and non-CNS), Store and Forward, Logon, and the parameters associated with each service.

Transport Addresses -- Lists each transport and the systems configured on each transport. The report identifies system areas and system IDs.

Device Addresses -- Lists each configured transport with the associated transport ID, the transport type, the data link processor (DLP) address and type, and the devices assigned to that DLP.

Transport Details -- Lists each configured transport and the transport's operating parameters. The report includes information specific to the transport type.

Service Windows -- Lists the configuration of each service window on the system. The report includes retries, time between retries, time between sessions, immediate priority postponement time, and the defined time intervals for each of the high, low, and medium priorities.

ACCESSING THE WSN CONFIGURATION REPORTER

To access the WSN Configuration Reporter, perform the following steps:

1. Log on to the VS. The Command Processor screen appears.

2. Press PF1, Run Program or Procedure. The Run screen appears.

3. Type WSNPRT as the program name. Specify the library and the volume where the WSNPRT program resides. The WSNPRT program resides in the library named @SYSCOM@. Press ENTER. The WSN Configuration Reporter menu appears (Figure 8-1).

```
15:13:05   ** WANG Systems Networking Configuration Reporter **   10/29/87
                Copyright, Wang Laboratories, Inc. 1987
                          Version 01.00.10

          Please select a reporting function from the list below:

                    (1)  Network Routing Summary
                    (2)  Service Summary  (↑ for System order)
                    (3)  Transport Addresses
                    (4)  Device Addresses
                    (5)  Transport Details
                    (6)  Service Windows

                   (10)  All reports
                   (15)  Display (↑ for previous report)
                   (16)  Exit
```

Figure 8-1. WSN Configuration Reporter Menu

From the WSN Configuration Reporter menu, you can press the appropriate PF key to generate a specific report, or you can press PF10 to generate all reports.

Generating a Report

When you select a report function, your screen displays the name of the report file being generated, as well as the name of the destination library and volume. Figure 8-2 shows a sample report processing screen for the Network Routing Summary.

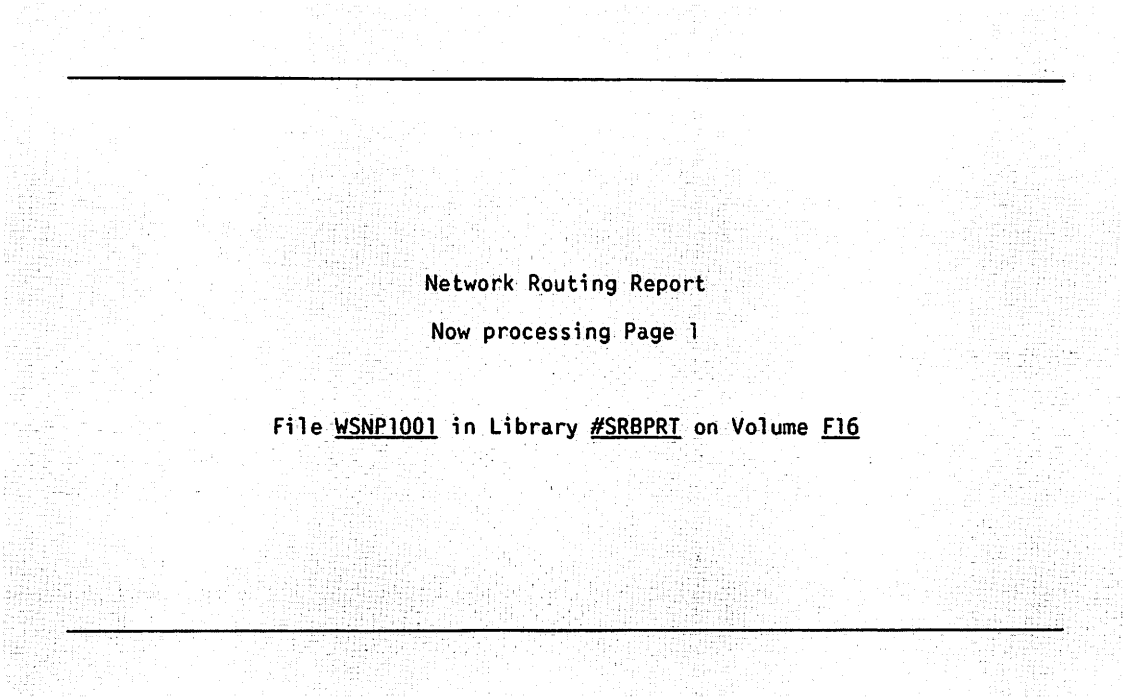

Figure 8-2. Sample Report Processing Screen

Report File Names

For each report function, the WSN Configuration Reporter creates a report of a specific file name, as follows:

Report Type	Report File Name
Network Routing Summary	WSNP1000
Service Summary	WSNP2000
Transport Addresses	WSNP3000
Device Addresses	WSNP4000
Transport Details	WSNP5000
Service Windows	WSNP6000

Each time you select a specific report function, the WSN Configuration Reporter increments the file name counter by 1. The counter is the last four numeric characters in the file name. For example, the first time you use the Network Routing Summary, the file is named WSNP1001; the next time you use the Network Routing Summary, the file is named WSNPRT1002, and so on. This allows you to create multiple reports without overwriting the previously created report of the same type.

Report File Storage

The WSN Configuration Reporter places your report files in the library named #___PRT. The blank spaces following the # sign are reserved for your 3-character logon ID. For example, if your logon ID is SRB, the report files are placed in the library named #SRBPRT on your system volume.

Printing a Report

When report processing is completed, a message on the screen requests a VS print mode for the report file. The VS print mode options appear on the Report Completed screen. Figure 8-3 shows a sample Report Completed screen.

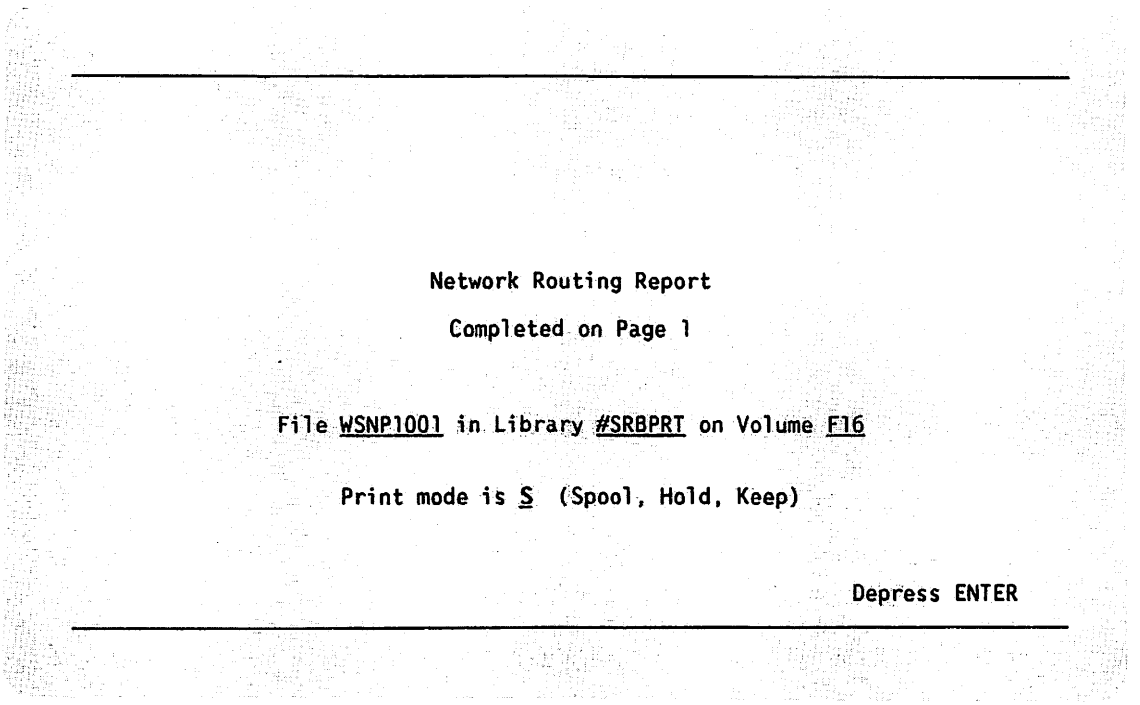

Figure 8-3. Sample Report Completed Screen

When the Report Completed screen appears, specify the VS print mode that you want to use by typing S (Spool), H (Hold), or K (Keep).

S (Spool) -- Sends the report file to the printer that is configured to your VS.

H (Hold) -- Holds the report file in the print queue until you release the file to the printer.

K (Keep) -- Stores the VS report file in the library/volume indicated on the Report Completed screen. The report file is not sent to the printer device.

Indicate the VS print mode and press ENTER to return to the WSN Configuration Reporter menu. The message "PRINTED" appears to the left of the report function that you selected.

Generating All Reports

If you want to generate all reports, press PF10. The WSN Configuration Reporter generates each report in sequence, starting with the Network Routing Summary. The VS print mode that you specify for the first report is used for ALL reports. As each report is generated, the PRINTED message appears to the left of the Report Type function on the menu. When all reports have been generated, you can display each report individually.

Displaying and Printing Reports

The WSN Configuration Reporter allows you to display reports after you create them. Press PF15 (Display) on the WSN Configuration Reporter menu to display the most recently generated report.

If you want to display a report that you created earlier, hold down the Shift key and press PF15. The latest report file names appear to the left of each report function on the menu. You can enter the name of the report that you want to display and press ENTER, or you can press PF15 (Display Next) to display each report in sequence.

Note: *Refer to the* WSN Network Configuration Guide *for a complete description of the fields that appear on each report.*

When a report is displayed, scrolling functions appear at the top of the report screen. These scrolling functions allow you to shift the report right, left, up, or down, so that you can scan the report for the information that you want to view. Table 8-1 lists the functions that appear at the top of a display screen.

Table 8-1. WSN Configuration Reporter Screen Functions

When You Press	You Can
PF1 (Menu)	Return to the WSN Configuration Reporter menu
PF3 (Position)	Display the current line and column position of the screen cursor
PF8 (Find)	Move the screen cursor to the start of a specified text string
PF9 (L Margin)	Shift the report right to display the left margin area of the report
PF10 (R Margin)	Shift the report left to display the right margin area of the report
PF11 (Left 15)	Shift the report right 15 columns
PF12 (Right 15)	Shift the report left 15 columns
PF13 (Left 1)	Shift the report right one column
PF14 (Right 1)	Shift the report left one column
PF15 (Print)	Display the Print Function Request menu to selectively print a range of report records or a range of report page numbers
PF16 (Exit)	Return to the WSN Configuration Reporter menu

From the currently displayed report, press PF15 (Print) to access the VS File Display Utility Print Function Request menu. This menu allows you to selectively print a range of report records, or a range of report pages. Figure 8-4 shows a sample Print Function Request menu.

```
*** Wang VS File Display Utility - Version 3.08.23 ***
 Print File WSNP1001 in Library #SRBPRT on Volume F16
  Contains      20 records of 134 bytes each maximum.

                  Print Function Request Menu

ENTER    -   Print the range of records described below
PF1      -   Return to displaying the file
PF2      -   Print the range of pages described below

Starting record number   -   ALL
Ending   record number   -

                - or -

Starting page   number   -   ALL
Ending   page   number   -

Note:  FIRST, LAST, and ALL are valid range delimiters.
```

Figure 8-4. Sample Print Function Request Menu

Enter the starting and the ending record number, or enter the starting and the ending page number in the 8-character fields, and then select a function as follows:

ENTER -- Print the range of records as specified on the menu
PF1 -- Redisplay the report on your screen
PF2 -- Print the range of pages as specified on the menu

ALL is the default range delimiter.

SAMPLE REPORTS

The WSN Configuration Reporter options are described in the following paragraphs. Figures 8-5 through 8-11 show sample reports.

Network Routing Summary

The Network Routing Summary report lists areas and systems to which paths have been defined. The report includes next hop systems, path costs, transports, and the base cost associated with each transport.

To generate the Network Routing Summary report, press PF1 from the WSN Configuration Reporter menu. The first time you generate the Network Routing Summary, it is named WSNP1000. Figure 8-5 shows a sample Network Routing Summary.

Service Summary

The Service Summary lists all systems and the services defined for each system. The report includes CNS, File Transfer (CNS and non-CNS), Store and Forward, Logon, and the parameters associated with each service.

To generate the Service Summary (by Area ID/System ID), press PF2 from the WSN Configuration Reporter menu. The first time you generate the Service Summary report, it is named WSNP2000. Figure 8-6 shows a sample Service Summary (by AID/SID).

To generate the Service Summary (by system order), press SHIFT and PF2 simultaneously. Press PF15; a north arrow (↑) appears next to the file name (to the left of the Service Summary function on the WSN Configuration Reporter menu), indicating that the report was created by system order. Figure 8-7 shows a sample Service Summary (by system order).

Transport Addresses

The Transport Addresses report lists each transport name, the transport type, and the systems configured on each transport. The report identifies system areas and system IDs.

To generate the Transport Addresses report, press PF3 on the WSN Configuration Reporter menu. The first time you generate the Transport Addresses report, it is named WSNP3000. Figure 8-8 shows a sample Transport Addresses report.

Device Addresses

The Device Addresses report lists each configured transport, the associated transport ID, the transport type, the data link processor (DLP) address and type, and the devices assigned to that DLP.

To generate the Device Addresses report, press PF4 on the WSN Configuration Reporter menu. The first time you generate the Device Addresses report, it is named WSNP4000. Figure 8-9 shows a sample Device Addresses report.

Transport Details

The Transport Details report lists each configured transport and the transport's operating parameters. The report includes information specific to the transport type.

To generate the Transport Details report, press PF5 on the WSN Configuration Reporter menu. The first time you generate the Transport Details report, it is named WSNP5000. Figure 8-10 shows a sample Transport Details report.

Service Windows

The Service Windows report lists the configuration of each service window on the local system. The report includes retries, time between retries, time between sessions, immediate priority postponement time, and the defined time intervals for each of the three priorities (high, low, and medium).

To generate the Service Windows report, press PF6 on the WSN Configuration Reporter menu. The first time you generate the Service Windows report, it is named WSNP6000. Figure 8-11 shows a sample Service Windows report.

09:16:59 Network Routing 11/06/87 Page 1

For system NETVS (SID = 2) in area AREATWO (AID = 2)

NCC is ATLAS (SID = 1) in area AREASEVEN (AID = 7) Network is RDALPHANETWORK

Destination				Path					Base	S&F Override		
System	Area	AID	SID	Next Hop	AID	SID	Cost	Transport	Cost	System	AID	SID
(All)	(Without path)			(None)						ATLAS	7	1
(All)	1AREATEST	1111		1IDS	1111	8888	2	IDS4TESTONLY	2			
(All)	AREA08AUSTRALIA	8		ATLAS	7	1	2	LOCAL5CABLE	2	ATLAS	7	1
								FFM4IN4TOWERTWO	4			
(All)	AREA27EUROPE	27		ATLAS	7	1	2	LOCAL5CABLE	2			
								FFM4IN4TOWERTWO	4			
(All)	AREA41TELENOVA	41		NOVA	41	1	2	ONETVSNOTPRIMARY	2			
(All)	AREA69EUROPE	69		ATLAS	7	1	2	LOCAL5CABLE	2			
								FFM4IN4TOWERTWO	4			
(All)	AREA70AUSTRALIA	70		ATLAS	7	1	2	LOCAL5CABLE	2	ATLAS	7	1
								FFM4IN4TOWERTWO	4			
(All)	AREAFIVE	5		DMFCNTRL	5	2	3	LOCAL5CABLE	2	UPTOWN	5	1
				UPTOWN	5	1	2	LOCAL5CABLE	2			
				VSNM	5	3	2	LOCAL5CABLE	2			
(All)	AREAFOUR	4		SNA90	4	1	2	LOCAL5CABLE	2	SNA90	4	1
(All)	AREANINENONCNS	9		LOCALNET	1	4	2	LOCAL5CABLE	2			
				ATLAS	7	1	3	LOCAL5CABLE	2			
								FFM4IN4TOWERTWO	4			
(All)	AREAONE	1		LOCALNET	1	4	2	LOCAL5CABLE	2	LOCALNET	1	4
				DUNE	1	22	2	LOCAL5CABLE	2			
(All)	AREAOSI	100		ATLAS	7	1	4	LOCAL5CABLE	2			
								FFM4IN4TOWERTWO	4			

Figure 8-5. Sample Network Routing Summary Report

09:18:00 Service Summary by AID/SID 11/06/87 Page 1

For system NETVS (SID = 2) in area AREATWO (AID = 2)

NCC is ATLAS (SID = 1) in area AREASEVEN (AID = 7) Network is RDALPHANETWORK

AID	SID	System	Area	System Type	ACC	Dist Pt.	CNS Inst	CNS FTM	S&F Inst	Services Logon	Services Transfer	Transfer Password	Transfer Group	Service Window
2	2	NETVS	AREATWO	VS			Y	Y	Y	X	X		DEFAULTXFGROUP	
1	1	ALFRED	AREAONE	VS			Y	Y	N					
1	4	LOCALNET	AREAONE	VS	A	D	Y	N	Y	X	X		DEFAULTXFGROUP	
1	22	DUNE	AREAONE	VS			Y	Y	Y	X	X			TEST2
1	99	TEST	AREAONE	VS			Y	Y	N					
2	1	OS11	AREATWO	VS	A	D	Y	N	Y	X	X		DEFAULTXFGROUP	
2	2	NETVS	AREATWO	VS			Y	Y	Y	X	X		DEFAULTXFGROUP	
2	12	BOK2	AREATWO	WPC			Y	Y	N	X	X			
3	3	VS1	AREATHREE	VS			Y	Y	Y					
3	4	VS80 _	AREATHREE	VS	A	D	Y	Y	Y					
3	5	VSTE	AREATHREE	VS			Y	Y	Y					
3	35	IDSR20T	AREATHREE	IDS			Y	N	Y	X	X			TEST2
4	1	SNA90	AREAFOUR	VS	A	D	Y	Y	Y	X	X		DEFAULTXFGROUP	
4	2	SNAKE	AREAFOUR	VS			Y	Y	Y					
4	3	SNA15	AREAFOUR	VS			Y	Y	Y					
5	1	UPTOWN	AREAFIVE	VS	A	D	Y	Y	Y	X	X		DEFAULTXFGROUP	
5	2	DMFCNTRL	AREAFIVE	VS			Y	Y	Y	X	X		DEFAULTXFGROUP	
5	3	VSNM	AREAFIVE	VS			Y	Y	Y	X	X		DEFAULTXFGROUP	
7	1	ATLAS	AREASEVEN	VS	A	D	Y	N	Y	X	X		DEFAULTXFGROUP	TEST3
8	8003	SPO100B1	AREA08AUSTRALIA	VS			Y	Y	Y					
8	8004	SPO85	AREA08AUSTRALIA	VS	A	D	Y	Y	Y		X		DEFAULTXFGROUP	
9	1	OISNM	AREANINENONCNS	OIS			N	N	N	X	X			
9	2	EEYORE	AREANINENONCNS	OIS			N	N	N	X	X	PASSWORD		
9	3	TRON	AREANINENONCNS	OIS			N	N	N	X	X			
9	4	JMTAB	AREANINENONCNS	OIS			N	N	N	X	X	PASSWORD		
9	5	OS2	AREANINENONCNS	OIS			N	N	N	X	X			
9	6	NETMGMT	AREANINENONCNS	OIS			N	N	N	X	X	PASSWORD	NETMGMT	
9	7	TIGGER	AREANINENONCNS	OIS			N	N	N	X	X			
9	11	SYS	AREANINENONCNS	OIS			N	N	N	X	X	PASSWORD		
9	100	PROBE	AREANINENONCNS	VS			N	N	N	X	X			
9	123	JUNK1	AREANINENONCNS	VS			Y	Y	N					
10	1	IDSR20G1	AREATEN	IDS			Y	N	Y	X	X			
10	4	VEGEMITE	AREATEN	VS			Y	Y	Y					
10	8	IDSR21F1	AREATEN	IDS			Y	N	Y	X	X			

Figure 8-6. Sample Service Summary Report (by AID/SID)

09:18:40 Service Summary by System 11/06/87 Page 1

For system NETVS (SID = 2) in area AREATWO (AID = 2)

NCC is ATLAS (SID = 1) in area AREASEVEN (AID = 7) Network is RDALPHANETWORK

AID	SID	System	Area	System Type	ACC	Dist Pt.	CNS Inst	CNS FTM	S&F Inst	Services Logon	Services Transfer	Transfer Password	Transfer Group	Service Window
2	2	NETVS	AREATWO	VS			Y	Y	Y	X	X		DEFAULTXFGROUP	
1111	1112	1111	1AREATEST	VS			Y	Y	N					
1111	1113	1113	1AREATEST	VS			N	N	N					
4444	1	114A	8023AREA	WPC			Y	Y	N					
1111	4444	12200	1AREATEST	2200			N	N	N					
1111	3333	1ALLIANC	1AREATEST	Alliance			N	N	N					
1111	2221	1FTM	1AREATEST	VS			Y	Y	N					
1111	8888	1IDS	1AREATEST	IDS			Y	Y	N	X	X	TEST		
1111	2223	1NOFTM	1AREATEST	VS			Y	N	N					
1111	1	1OIS	1AREATEST	OIS			N	N	N					
1111	2222	1VS	1AREATEST	VS			Y	N	N					
1111	6666	1WOA	1AREATEST	WOA			N	N	N					
1111	5555	1WPC	1AREATEST	WPC			Y	N	N					
1111	2224	2FTM	1AREATEST	VS			Y	N	N					
1111	2225	2NOFTM	1AREATEST	VS			Y	N	N					
1111	3	3	1AREATEST	VS			Y	Y	N					
1	1	ALFRED	AREAONE	VS			Y	Y	N					
7	1	ATLAS	AREASEVEN	VS	A	D	Y	N	Y	X	X		DEFAULTXFGROUP	TEST3
70	1	ATSYDNEY	AREA70AUSTRALIA	VS	A	D	Y	Y	Y		X		DEFAULTXFGROUP	TEST3
100	3	B52	AREA0SI	VS			Y	N	N					
15	1	BOK	AREAFIFTEEN	WPC			N	N	N	X	X			
2	12	BOK2	AREATWO	WPC			Y	Y	N	X	X			
10	18	COBBER	AREATEN	VS			Y	Y	Y	X	X			
41	2	COMET	AREA41TELENOVA	VS			Y	Y	Y					
27	3	DEMV01	AREA27EUROPE	VS			Y	Y	Y	X				
27	2	DEMV02	AREA27EUROPE	VS			Y	Y	Y	X				
10	17	DIGGER	AREATEN	VS			Y	Y	Y	X	X			
5	2	DMFCNTRL	AREAFIVE	VS			Y	Y	Y	X	X		DEFAULTXFGROUP	
1	22	DUNE	AREAONE	VS			Y	Y	Y	X	X			TEST2
27	5	EBC01	AREA27EUROPE	VS			Y	Y	Y	X				
9	2	EEYORE	AREANINENONCNS	OIS			N	N	N	X	X	PASSWORD		
1111	1234	GOOMBA	1AREATEST	VS			Y	Y	N					
1111	1235	GOOMBSNA	1AREATEST	VS			Y	Y	N					
10	1	IDSR20G1	AREATEN	IDS			Y	N	Y	X	X			

Figure 8-7. Sample Service Summary Report (by System Order)

09:19:26 Transport Addresses 11/06/87 Page 1

For system NETVS (SID = 2) in area AREATWO (AID = 2)

The system is configured with 15 transports

Transport	TID	Type	System	Address	Area	AID	SID
ONETVSNOTPRIMARY	3	WSN Multipoint	NETVS	02	AREATWO	2	2
			NOVA	01	AREA41TELENOVA	41	1
BOKLINK	5	WSN P-P Leased	BOK		AREAFIFTEEN	15	1
			NETVS		AREATWO	2	2
DIALANOTHERTIME	6	WSN P-P Switched	BOK2	73642	AREATWO	2	12
			NETVS	72153	AREATWO	2	2
DIALUPOS11	7	WSN P-P Switched	NETVS	72946	AREATWO	2	2
FAM4INTOWER4TWO _	8	WSN P-P Switched	NETVS	1006	AREATWO	2	2
FFM4IN4TOWERTWO	9	WSN P-P Leased	ATLAS		AREASEVEN	7	1
			NETVS		AREATWO	2	2
IDS4BSC4SAMPLE	10	IDS 3271 (BSC)	IDSR20T		AREATHREE	3	35
			IDSR21F1		AREATEN	10	8
			NETVS		AREATWO	2	2
IDS4SNA4SAMPLE	11	IDS 3274 (SNA)	IDSR20G1		AREATEN	10	1
			IDSR20T		AREATHREE	3	35
			IDSR21F1		AREATEN	10	8
			NETVS		AREATWO	2	2
IDS4TESTONLY	12	IDS 3271 (BSC)	1IDS		1AREATEST	1111	8888
			NETVS		AREATWO	2	2
LD1208	13	WSN P-P Leased	1208		(Not Defined)	0	0
			NETVS		AREATWO	2	2
LOCAL5CABLE	14	WSN Wangband	ATLAS	0A21	AREASEVEN	7	1
			COBBER	0A18	AREATEN	10	18
			DIGGER	0A17	AREATEN	10	17
			DMFCNTRL	0056	AREAFIVE	5	2

Figure 8-8. Sample Transport Addresses Report

09:19:53 Device Addresses 11/06/87 Page 1

For system NETVS (SID = 2) in area AREATWO (AID = 2)

The system is configured with 15 transports

Transport	TID	Type	DLP	Type	Devices	Speed
ONETVSNOTPRIMARY	3	WSN Multipoint	Invalid DLP address			
BOKLINK	5	WSN P-P Leased	000K	TCB1	011-013	19200
DIALANOTHERTIME	6	WSN P-P Switched	000J	TCB1	008-010	4800
DIALUPOS11	7	WSN P-P Switched	000I	TCB1	006-007	4800
FAM4INTOWER4TWO	8	WSN P-P Switched	Invalid DLP address			
FFM4IN4TOWERTWO	9	WSN P-P Leased	000L	TCB1	016-019	9600
IDS4BSC4SAMPLE-	10	IDS 3271 (BSC)	N/A			
IDS4SNA4SAMPLE	11	IDS 3274 (SNA)	N/A			
IDS4TESTONLY	12	IDS 3271 (BSC)	N/A			
LD1208	13	WSN P-P Leased	144D	TCB3	156-159	64000
LOCAL5CABLE	14	WSN Wangband	176A	CIU	176-183	
SHORT	15	WSN Multipoint	000N	TCB1	020-023	64000
TELENETSAMPLE	16	X25 WANGPAC	Invalid DLP address			
TESTFORWSNPRT	77	X25 WANGPAC	Invalid DLP address			
WPCLOCAL4SAMPLE	19	PC Local Option	144B	TCB3	148-151	

Figure 8-9. Sample Device Addresses Report

```
09:20:07                    Transport Details                    11/06/87                    Page 2
          For system NETVS (SID = 2) in area AREATWO (AID = 2)

               The system is configured with 15 transports

BOKLINK                                                                          BOKLINK

    Transport Name  BOKLINK              Electrical Interface  RS232
      Transport Id  5                       Line Duplex Mode  Full
    Transport Type  WSN P-P Leased              Line Speed  19200
       DLP Address  000K
          DLP Type  TCB1
           Devices  011-013
         Base Cost  1
    Initial Status  Disabled
Inactivity Timeout  30 (sec)
Reactivation Timer  300 (sec)
   Connection Bias  2
 Congestion Levels  2, 4, 6, 8

09:20:07                    Transport Details                    11/06/87                    Page 4
          For system NETVS (SID = 2) in area AREATWO (AID = 2)

               The system is configured with 15 transports

DIALUPOS11                                                                       DIALUPOS11

    Transport Name  DIALUPOS11           Electrical Interface  RS232
      Transport Id  7                       Line Duplex Mode  Half
    Transport Type  WSN P-P Switched            Line Speed  4800
       DLP Address  0001                     Call Direction  Both
          DLP Type  TCB1                 Manual Dial Timeout  2 (min)
           Devices  006-007
         Base Cost  8                     Disconnect Timeout  60 (sec)
    Initial Status  Enabled               Autocall Unit Type  None
Inactivity Timeout  30 (sec)                  Dialer Address
Reactivation Timer  300 (sec)                  Modem Address
   Connection Bias  2                       Dial Retry Count
 Congestion Levels  2, 4, 6, 8              Dial Retry Time
```

Figure 8-10. Sample Transport Details Report

```
09:20:32                    Service Windows                11/06/87                    Page 1
          For system NETVS (SID = 2) in area AREATWO (AID = 2)

               The system is configured with 3 windows


TEST2                                                        TEST2


                          Window Name:  TEST2

          Maximum Number of Retries:  3
              Time Between Retries:  00 : 15 (hh : mm)

             Time Between Sessions
             within an Open Window:  00 : 15 (hh : mm)

                 Immediate Priority
                  postponement time:  00 : 15 (hh : mm)

                            Service Window
                                 for
    Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Priority                        Time: AM

       12__ 1___ 2___ 3___ 4___ 5___ 6___ 7___ 8___ 9___ 10__ 11__
High   ____ ____ ____ ____ ____ ____ ____ ____ XXXX XXXX XXXX XXXX
 Med   ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____
 Low   XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX ____ ____ ____ ____

Priority                        Time: PM

       12__ 1___ 2___ 3___ 4___ 5___ 6___ 7___ 8___ 9___ 10__ 11__
High   XXXX XXXX XXXX XXXX XXXX ____ ____ ____ ____ ____ ____ ____
 Med   ____ ____ ____ ____ ____ XXXX XXXX XXXX XXXX XXXX XXXX ____
 Low   ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ XXXX
```

Figure 8-11. Sample Service Windows Report

APPENDIX A
LOGGER SUBSYSTEM IDENTIFIERS

This appendix lists the logger subsystem identifiers that you can specify with the Event Inquiry Facility. The PF9 (Respecify) function allows you to change the current criteria to display the messages associated with your local system's activity in connecting to a specific system or subsystem.

Table A-1 lists the logger subsystem identifiers, the associated subsystems, and their descriptions.

Table A-1. Logger Subsystem Identifiers

Subsystem ID	Subsystem Name	Description
000	ALL subsystems	
064	SNAMON	SNA Monitor
067	WBMF	Wang Band Management Facility
069	CNS	CNS
070	CNSMON	CNS Monitor
071	CNSMGR	CNS Manager
084	SoftMgr	Software Manager
090	NetBakup	VS Network Backup Facility
091	SYSMON	System Monitor
093	ILS	Incident Logging System
096	WANMGR	Wide Area Network Manager
097	8023MGR	IEEE 802.3 Manager

(continued)

Table A-1. Logger Subsystem Identifiers (continued)

Subsystem ID	Subsystem Name	Description
099	DMF-EXEC	Distributed Management Facility
101	S&F	Store and Forward
110	TCP/IP	TCP/IP
111	X29	Network Terminal Server - X.29
128	OFFICE	Wang OFFICE/S&F/Audit Trails
145	WSN FTM	WSN File Transfer Manager
146	DIRSYNC	Directory Synchronization
148	CNXMGR	Connection Manager
176	IOPMGR	IOP Manager
255	LOGGER	DMF/NETCORE Logger

APPENDIX B
LOG MESSAGES, REASON CODES, AND DLP CODES

INTRODUCTION

When you press PF17 from any CNS Manager screen, the CNS Manager links to the Event Inquiry Facility. The Event Inquiry Facility allows you to view network activity messages as they are written to the log. These messages are explained in this appendix.

CNS LOG MESSAGES

The Event Inquiry Facility screen displays messages about the status of CNS applications, transports, and data transfers. These log messages are recorded in the daily log files that reside in the library named @LOG@.

Each file in @LOG@ contains log messages that were generated for a given day. A new file is created for each new 24-hour period; the name of the file is in the format, Lyymmdd (where yy = year, mm = month, and dd = day).

Log messages are passed to the Event Inquiry Facility by the background task $LOGTSK$. Log messages are presented in the format WSNxxnn, (where xx indicates the CNS layer that generated the message, and nn indicates the specific message). Within a given log message, there may appear a reason code in the format Reason = XX (where XX indicates the reason for the logging of the message).

There are six kinds of CNS messages that can appear on the Event Inquiry Facility screen, as described below:

Type	Description
WSN01	Global messages. Concern functions that are common to all CNS layers (for example, statistics gathering, network monitoring, application attachment, and the control of network resources).

Type	Description
WSN02	End-to-End layer messages. Concern the CNS End-to-End layer establishment; maintenance and termination of sessions; the sequencing, acknowledgment, and/or retransmission of data; and the prioritization of data flow.
WSN03	Switching layer messages. Concern the CNS Switching layer network evolution (XID exchange), route selection, lost path/message detection, and transport control.
WSN04	Transport layer messages. Concern the CNS transport delivery of Network Transfer Units (NTUs) across the physical link and the local Switching layer, and the status of the Physical layer.
WSN05	IDS messages. Generated by the CNS IDS Bisync and SNA Transport Drivers.
WSN06	GML 802.3 Link Driver messages. Generated by the Generic Message layer (GML); the messages appear in the log files with WSN VS NETCORE 8.32.

Global Log Messages (WSN01)

Global log messages are presented in the form WSN01nn (where nn reflects the specific message).

nn	Meaning
01	CNS VERSION [version number] HAS BEEN STARTED ON SYSTEM [system name], SYSID = [System ID], AREAID = [Area ID] CNS has been submitted to the background/foreground, most probably by running WSNSTART.
02	CNS TERMINATED NORMALLY BY OPERATOR CNS was brought down by the running of WSNSTOP.
07	APPLICATION ATTACHED, APPL = [application name], USER = [VS Logon ID], MAXSESSIONS = [#] An application has successfully attached to CNS. An application must be attached to CNS before it can communicate over the network.

nn	Meaning
08	APPLICATION DETACHED, APPL = [application name], USER = [VS Logon ID], SESSIONS IN = [#], SESSIONS OUT = [#], MESSAGES IN = [#], MESSAGES OUT = [#], BYTES IN = [#], BYTES OUT = [#], SUBTASK ID = [dynamic #] An application voluntarily detached itself from CNS after completing all of its sessions to one or more remote applications (for example, DIRSYNC detaches from CNS after completing Directory Synchronization).
09	APPLICATION ABNORMALLY TERMINATED, APPL = [application name], USER = [VS Logon ID], SESSIONS IN = [#], SESSIONS OUT = [#], MESSAGES IN = [#], MESSAGES OUT = [#], BYTES IN = [#], BYTES OUT = [#], REASON = [#/description], STID = [STS Subtask ID] For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
10	ATTACH FAILED, APPL = [application name], USER = [VS Logon ID], REASON = [#/description] For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
11	GETHEAP ERROR, BUFFERS MAY HAVE BEEN DISCARDED Insufficient segment 2 space is available for the CNS background task. For WSN VS NETCORE 8.32, 2048K is the minimum segment 2 space. The message may also indicate heavy CNS activity.
12	CNS CANCELLED BY OPERATOR, DUMPLIB = [library name], DUMPVOL = [volume name] The CNS task was cancelled from the Operator's Console. The message also appears when CNS is running as a foreground task and is cancelled.
13	CNS CANCELLED DUE TO PROGRAM CHECK, PCW = [PCW], DUMPLIB = [library name], DUMPVOL = [volume name] Save the dumpfile for analysis if this message continues to appear.

nn	Meaning
14	CNS PROCESSING TERMINATED, DUMPLIB = [library name], DUMPVOL = [volume name], RETURN CODE = [#/description] For possible return code values, see the section entitled "Subtask Scheduler (STS) Reason Codes."
15	APPLICATION [application name] SUCCESSFULLY SUBMITTED AS FILE [file name] IN LIBRARY [library name] ON VOLUME [volume name] An application was auto-started based on information in the associated application record in the Network Directory file. The message also appears when a CNS application is started manually.
16	APPLICATION [application name] UNSUCCESSFULLY SUBMITTED FROM FILE [file name] IN LIBRARY [library name] ON VOLUME [volume name] A CNS application cannot be run by the Operating System as a background procedure. The reason could be disk/volume related (such as VTOC errors, or the library is not on the specified volume). It may also be that a background task is not available, or the application is not listed in the Network Directory file.
17	APPLICATION [application name] NOT SUBMITTED, REASON = DIRECTORY LOOKUP FAILURE An application record does not exist in the Network Directory file for the specified application. An application can be added through Wang OFFICE Administrative Functions (Directory) or the WSNAPPS program.
20	OPEN/CREATE OF CNSLOG(nn) ON [volume name] IS (SUCCESSFUL/UNSUCCESSFUL) If creation is unsuccessful, it may be due to lack of sufficient disk space. If open is unsuccessful, the file may be damaged.

nn	Meaning
22	DIRECTORY COULD NOT BE ACCESSED BY NODE MGR, FUNCTION = [name of CNS configuration access routine], ERROR CODE = [return code from above-mentioned routine] The CNS Node Manager has a problem accessing the network directory. Use the Wang OFFICE Administrative Function of Directory or the WSNAPPS program to verify that the application records in the network directory file can be accessed successfully.
23	UNABLE TO SAVE CNS TRACE POINT FILE FOR NEXT RUN OF CNS CNS is unable to open/read the file CNTRACE in library @CNTRACE, and so is unable to obtain the information within. (This includes the current trace point settings, volume location and file size of the CNSLOG(nn) file.)
24	MSG LOGGED FOR USER [VS Logon ID], MSG = [message text] A user logged a message using CNSMGR.
25	CNS TRACE TABLE MODIFIED BY USER [VS Logon ID] Modification took place using CNSMGR.
26	(ENABLE/DISABLE) OF TRANSPORT [transport name] REQUESTED BY USER [VS Logon ID] Transport enable/disable took place using WSNMON/CNSMGR.
27	TRANSPORT COST(S) AND/OR TIMER VALUE(S) CHANGED BY USER [VS Logon ID] The Base Cost and/or Reactivation Timer value for a transport was modified using CNSMGR.
28	PATH COST(S) TO AREA = [Area ID], SYSTEM = [System ID] MODIFIED BY USER [VS Logon ID] Modification took place using WSNMON/CNSMGR.

nn	Meaning
29	LOGTSK DID NOT RESPOND. LOG MESSAGES LOST A message was not written to the log file because $LOGTSK$ was not running when CNS attempted to write the message, or because of heavy logging activity (that is, more records are being presented than $LOGTSK$ can process).
30	CONNECTION MANAGER DOES NOT RESPOND. AUTOSTART REQUESTS ARE FORWARDED TO THE NODE MANAGER. The CNS Node Manager is unable to communicate with @CNXMGR@. The CNS Node Manager attempts to submit any autostart application attach requests to CNS which would otherwise be submitted by @CNXMGR@. It is consequently possible that not all attach requests will be honored.
31	UNABLE TO CREATE ITM PORT @CNR FOR CNXMGR AUTOSTART RESPONSES CNS is unable to create the necessary intertask message port that would enable it to communicate with the Connection Manager.
32	SESSION TERMINATED AT REQUEST OF OPERATOR, SID = [End-to-End Layer session ID] An IWSCORE session was terminated.
33	CONNECTION MANAGER NOT ACTIVE @CNXMGR@ is not executing in the background. It may have crashed (check for a task dump), or it may have been brought down by a user. @CNXMGR@ is submitted to the background through WSNSTART.

End-to-End Layer Log Messages (WSN02)

End-to-End layer log messages are presented in the form WSN02nn (where "nn" reflects the number of the specific message expressed in decimal form).

nn	Meaning
01	SESSION RETRANSMISSION LIMIT EXCEEDED, SID = [local End-to-End Layer session ID] The destination system or an intermediate system in a multihop path may have a problem. Check the status of the remote system, CNS, etc.
02	APPLICATION DETACHED, APPL = [application name], USER = [VS Logon ID], SESSIONS IN = [#], SESSIONS OUT = [#], MESSAGES IN = [#], MESSAGES OUT = [#], BYTES IN = [#], BYTES OUT = [#] Same as global log message WSN0108.
03	APPLICATION ABNORMALLY TERMINATED, APPL = [application name], USER = [VS Logon ID], SESSIONS IN = [#], SESSIONS OUT = [#], MESSAGES IN = [#], MESSAGES OUT = [#], BYTES IN = [#], BYTES OUT = [#], REASON = [#/description] Same as global log message WSN0109.
04	INBOUND SESSION ESTABLISHED, SID = [local End-to-End layer session ID], LOCAPPL = [application name], USER = [VS Logon ID], REMAPPL = [application name], REMSYSID = [System ID], REMAREAID = [Area ID], APPLSID = [NAI/Application layer session ID], PRIORITY = [#] A session was initiated with a local application by a remote application.
05	OUTBOUND SESSION ESTABLISHED, SID = [local End-to-End layer session ID], LOCAPPL = [application name], USER = [VS Logon ID], REMAPPL = [application name], SYSTEM = [system name], APPLSID = [NAI/Application layer session ID], PRIORITY = [#] A session was initiated by a local application with a remote application.

nn	Meaning
06	INBOUND SESSION REJECTED, SID = [local End-to-End layer session ID], LOCAPPL = [application name], REMAPPL = [application name], SYSTEM = [system name], REASON = [#/description] An application at a remote system attempted to establish a session with an application on the local system. The session may have been rejected due to a failure to find the local application. For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
07	OUTBOUND SESSION REJECTED, SID = [local End-to-End layer session ID], LOCAPPL = [application name], REMAPPL = [application name], SYSTEM = [system name], REASON = [#/description] An application on the local system could not establish a session with an application at a remote system due to a directory look-up failure. The local application could not be found in the directory. For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
08	SESSION TERMINATED NORMALLY, SID = [local End-to-End layer session ID], USER = [VS Logon ID], MSGS IN = [#], MSGS OUT = [#], BYTES IN = [#], BYTES OUT = [#], REXMITS OUT = [#], REXMITS IN = [#], RCVD OUT OF SEQ = [#] A session was completed. If there were many REXMITS, check the transports along the probable route. If there were many RCVD OUT OF SEQ messages, check the route definition to verify that messages are taking the correct route.
09	SESSION TERMINATED ABNORMALLY, SID = [local End-to-End layer session ID], User = [VS Logon ID], MSGS IN = [#], MSGS OUT = [#], BYTES IN = [#], BYTES OUT = [#], REXMITS OUT = [#], REXMITS IN = [#], RCVD OUT OF SEQ = [#], REASON = [#/description] A session has been terminated abnormally (before a close request has been sent and acknowledged). Possible reasons include a line failure, insufficient resources at a system, a system failure, etc. For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
10	SYSTEM [system name] HAS BEEN CONTACTED The End-to-End layers on the source and destination systems have successfully exchanged End-to-End layer revision levels.

nn	Meaning
11	END TO END RESTART FAILURE WITH SYSTEM [system name], LOCALREV = [#], REMREV = [#], REASON = [#/description] End-to-End layer revision level exchange between the source and destination system was unsuccessful. For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
12	INCOMPATIBLE SYSTEM NAMES ON RESTART, EXPECTED = [remote system name from local Network Directory file], ACTUAL = [remote WangNet ID] Use the WSNEDIT utility to verify/reconfigure the remote system into the Network Directory file and the network COMFIG file. A system IPL is necessary after reconfiguration.
13	CONTACT HAS BEEN LOST WITH SYSTEM [system name], REASON = [#/description] For possible reason values, see the section entitled "End-to-End Layer Reason Codes."
14	SYSTEM [system name] HAS BEEN RESTARTED CNS was restarted (brought down, then brought back up) on an adjacent system after the local system had established a link.
15	INBOUND CONNECT REQUEST RECEIVED, SID = [local End-to-End layer session ID], LOCAPPL = [application name], REMAPPL = [application name], SYSTEM = [remote system name]
16	OUTBOUND OPEN ACCEPT SENT FROM LOCAL APPLICATION, APSESID = [NAI/Application Layer session ID], NETSESID = [End-to-End layer session ID of remote session], DESTSYSTEM = [system name]
17	EE: UNKNOWN REQUEST FROM [CNS component name] RCVD BY END-END LAYER, REQ TYPE = [#]

Switching Layer Log Messages (WSN03)

Switching layer log messages are presented in the form WSN03nn (where nn reflects the number of the specific message expressed in decimal form).

nn	Meaning
01	ENABLING TRANSPORT [transport name] The Switching layer is enabling a transport. After a transport is enabled, it is available for CNS data transfer. A transport can be enabled through use of the CNS Manager. The Switching layer also enables a transport each time CNS is submitted to the background and the transport has an initial WSNEDIT status of ENABLE.
02	DISABLING TRANSPORT [transport name] The Switching layer is disabling a transport. After a transport is disabled, it is not available for CNS data transfer (although it is still available for use by non-CNS applications). A transport can be disabled by use of WSNMON/CNSMGR, or by CNS in the case of a transport failure. If the link is physically down, use the CNS Manager to disable the transport.
03	TRANSPORT [transport name] ENABLED The Switching layer successfully enabled the transport.
04	TRANSPORT [transport name] DISABLED The Switching layer successfully disabled the transport.
05	ROUTE RE-ENABLED TO SYSTEM [System ID], AREA [Area ID] USING TRANSPORT [transport name] See entry WSN0306 for an explanation.
06	ROUTE DISABLED TO SYSTEM [System ID], AREA [Area ID] USING TRANSPORT [transport name], REASON = [#/description] When the Switching layer is unsuccessful in exchanging XIDs with an adjacent system, the link is disabled for 30 seconds. If an undeliverable message is received from the Transport Driver for that link and multiple transports are configured between the two systems, the transport is disabled for the time specified in the WSNEDIT Reactivation Timer field. The temporarily disabled state is logged as WSN0306. When the link/route is re-enabled, it is logged as WSN0305. For possible reason values, see the section entitled "Switching Layer Reason Codes."

nn	Meaning
07	CNS REVISION LEVEL HAS BEEN SUCCESSFULLY EXCHANGED WITH SYSTEM [System ID], AREA [Area ID], LOCALREV = [#], REMOTEREV = [#] The Switching layers on the local and adjacent systems have successfully exchanged Switching layer revision levels.
08	CNS REVISION LEVEL HAS BEEN UNSUCCESSFULLY EXCHANGED WITH SYSTEM [System ID], AREA [Area ID], LOCALREV = [#], REMOTEREV = [#], REASON = [#/description] Switching layer revision level exchange between the local and adjacent systems was unsuccessful. The local system's attempt to exchange XID commands with an adjacent system has been unsuccessful. Adjacent systems cannot communicate, nor can one send data through another to a destination, until they exchange XID commands. These commands identify the CNS revision levels that are installed on the systems. Systems with the same revision level can communicate. Systems with different revision levels can communicate if one revision level is the immediate successor of the other. For possible reason values, see the section entitled "Switching Layer Reason Codes."
09	INSUFFICIENT ENDPOINT ROUTING INFORMATION: NO DEFAULT PATH SUPPLIED Use the WSNEDIT utility to check the default routing path information.
10	UNABLE TO CREATE TRANSPORT SUBTASK An attempt was made to configure and enable more than 29 CNS transports on the local system.
12	PROTOCOL VIOLATION INBOUND, COMMAND = [#], REASON = [#/description] The command passed from the Transport layer to the Switching layer was unintelligible to the Switching layer. For possible reason values, see the section entitled "Switching Layer Reason Codes."

nn	Meaning
13	PROTOCOL VIOLATION OUTBOUND, COMMAND = [#], REASON = [#/description] The command passed from the End-to-End layer to the Switching layer was unintelligible to the Switching layer. For possible reason values, see the section entitled "Switching Layer Reason Codes."
14	MESSAGE DISCARDED, SYSTEM = [system name], SUBTASK ID = [dynamic #], REASON = [#/description] For possible reason values, see the section entitled "Switching Layer Reason Codes."
15	PATH REJECT RECEIVED FOR SYSTEM [System ID], AREA [Area ID], REJECTING SYSTEM [System ID], AREA [Area ID], REASON = [#/description] For possible reason values, see the section entitled "Switching Layer Reason Codes."
16	UNDELIVERABLE RECEIVED FOR SYSTEM [System ID], AREA [Area ID], FROM ADJACENT SYSTEM [System ID], USING TRANSPORT [transport name], REASON = [#/description] For possible reason values, see the section entitled "Switching Layer Reason Codes."
17	ROUTE CONFIRM GENERATED; DESTINED FOR SYSTEM [System ID], AREA [Area ID], ON LINK [transport name]
18	MESSAGE DISCARDED, SOURCE SYS = [System ID], SOURCE AREA = [Area ID], DEST SYS = [System ID], DEST AREA = [Area ID], REASON = [#/description] This message is logged on an intermediate system when the hop count is 0 or when there are no enabled, nonblocked transports back to the source system on which to return an Undeliverable or Path Reject message. For possible reason values, see the section entitled "Switching Layer Reason Codes."

nn	Meaning
19	MESSAGE DISCARDED, SUBTASK ID = [dynamic #], REASON = [#/description] The STS Subtask ID is invalid. This is an internal error. For possible reason values, see the section entitled "Switching Layer Reason Codes."
20	ROUTE BY NAME ERROR, REASON = [#/description] For possible reason values, see the section entitled "Switching Layer Reason Codes."

Transport Layer Log Messages (WSN04)

Transport Driver log messages are presented in the form WSN04nn (where nn reflects the number of the specific message expressed in decimal form).

nn	Meaning
01	UNABLE TO READ CONFIGURATION ON LINK [transport name], REASON = [#] The local view configuration file could not be read. The file is missing, or it is probably not on the IPL volume. The decimal value for # and the corresponding meaning for each are as follows:

Decimal Value for #	Meaning
04	SUCCESSFUL (data truncated due to lack of space)
08	CONNECTION NOT POSSIBLE (invalid protocol or protocol ID for CONNECT or LINKDATA)
12	INVALID SERVICE OR SERVICE NODE
16	INVALID NODE OR NODE ID
20	INVALID LINK OR LINK ID
24	NODE NOT CONFIGURED FOR SERVICE
28	INVALID FUNCTION IN PARAMETER LIST
32	AREA OR LENGTH OPERAND INVALID
36	NO CONFIGURATION (FILE) AVAILABLE
40	LINK INITIALIZATION NOT POSSIBLE (no local node or not on link)

Decimal Value for #	Meaning
44	CONFIGURATION FILE INCONSISTENT (search key not found)
48	DLP DOES NOT EXIST IN SYSGEN
52	HEADER RECORD DOESN'T EXIST

nn **Meaning**

02 UNABLE TO CONNECT TO SESSION MANAGER ON LINK [transport name], REASON = [#/description]

The transport cannot connect to the Session Manager. Transports must be able to connect to the Session Manager before they can support sessions. Verify that @SESMGR@ is running. For possible reason values, see the section entitled "Transport Driver Reason Codes."

03 UNABLE TO ESTABLISH TRANSPORT CONNECTION TO SYSTEM [system name] ON LINK [transport name], REASON = [#/description], CAUSE = [#], DIAGNOSTIC = [#]

A transport connection could not be established with an adjacent system. The DLP at the adjacent system is probably not running, or there are problems with the transport software.

For possible reason values, see the section entitled "Transport Driver Reason Codes." For possible cause and diagnostic values, contact your Wang customer representative.

04 TRANSPORT CONNECTION ESTABLISHED WITH SYSTEM [system name] ON LINK [transport name], DIRECTION = [INBOUND/OUTBOUND], DEVICE = [VSDN]

For possible direction values, see the section entitled "Transport Driver Directions."

05 TRANSPORT CONNECTION NORMALLY TERMINATED WITH SYSTEM [system name] ON LINK [transport name], DIRECTION = [INBOUND/OUTBOUND], DEVICE = [VSDN], DURATION = [# seconds]

The physical connection with the adjacent system was dropped. A connection is normally dropped when there are no CNS sessions pending and the Inactivity Timer (set with WSNEDIT) has expired.

nn	Meaning
06	TRANSPORT CONNECTION ABNORMALLY TERMINATED WITH SYSTEM [system name] ON LINK [transport name], REASON = [#/description], DIRECTION = [INBOUND/OUTBOUND], DEVICE = [VSDN], DURATION = [# seconds], DATA = [IOSW, UIOSW, or 8 bytes, 3 of which are from the Terminate/Suspend a Session SMXM ITM from @SESMGR@]

The transport connection was terminated abnormally, possibly because of a DLP failure on either the local or an adjacent system, a transport microcode failure, a line failure, or a system failure. When DATA contains the SMXM ITM, the format of DATA is as follows:

Byte	Meaning
0-3	Reserved
4	Cause byte
5	Always hex 03
6	Reserved
7	Diagnostic code

For a list of possible Cause Byte and Diagnostic Code values, contact your Wang customer representative. For possible reason values, see the section entitled "Transport Driver Reason Codes."

07	ATTEMPTING CONNECTION TO SYSTEM [system name] ON LINK [transport name], DEVICE = [VSDN]

IDS Log Messages (WSN05)

IDS log messages are presented in the form WSN05nn (where nn reflects the number of the specific message expressed in decimal form).

nn	Meaning
01	LINK [transport name] SUBMITTING MCP AS [file name] IN [library name] ON [volume name]

A transport driver submitted a procedure to run MCP as a background task. This happens if no MCP task was previously running. The message is logged with the file, library, and volume names blank when no procedure is specified in the WSNEDIT configuration of the transport and no MCP task is running.

nn	Meaning
02	LINK [transport name] UNABLE TO ATTACH DEVICE [LU # as defined in SNAEDIT] TO MCP, REASON = [#/description] The send/receive device (as specified in WSNEDIT) could not attach to MCP. Run VWS and try to attach with the LU number identified in the log message. For possible reason values, see the section entitled "IDS Reason Codes."
03	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] LOGGED ON TO CICS
04	LINK [transport name] RECEIVED UNEXPECTED MESSAGE, MESSAGE = [message text] A message was received from the host that does not begin with "W20." The message was not recognized. The message may be a broadcast message.
05	LINK [transport name] ATTEMPTING SELF-ENABLE The link was disabled and is attempting to enable itself. This might occur if MCP is suddenly not executing or if CICS went down; the link is disabled before attempting a self-enable.
06	LINK [transport name] SIGNED-ON TO IDS
07	LINK [transport name] INACTIVE, REASON = [#/description] For possible reason values, see the section entitled "IDS Reason Codes."
08	LINK [transport name] SIGNED-OFF OF IDS
09	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] 2ND SIGNON COMPLETE
10	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] LOGGED OFF OF CICS

nn	Meaning
11	LINK [transport name] ACTIVATION LEVEL DROP (CICS WENT DOWN, OR LINE HIT) ON DEVICE [LU # as defined in SNAEDIT], ATTEMPTING RECOVERY
12	LINK [transport name]. THIS IDS TRANSPORT TYPE IS NOT AVAILABLE ON THIS SYSTEM. The IDS transport microcode files do not exist on this system, or the files have been corrupted. Look for @MCIB06@ (for IDS Bisync) and @MCIST1@ (for IDS SNA transport), and delete/rename the files. Reload the good files.
13	LINK [transport name] DISABLED, REASON = [#/description] For possible reason values, see the section entitled "IDS Reason Codes."
14	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] DETACHED FROM MCP
15	LINK [transport name] ENABLE COMMAND RCVD DURING DISABLE PROCESSING. CMD IGNORED. The link was disabling itself when it received an ENABLE command and ignored it. Wait for the disable to complete and then reissue the ENABLE command.
16	LINK [transport name] ENABLE COMMAND RCVD DURING ENABLE PROCESSING. CMD IGNORED.
17	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] ATTACHED TO MCP
18	LINK [transport name] NOT COMPATIBLE WITH INSTALLED MCP, NEED SNAMCP 2.50.00 OR LATER Install a newer release of SNA software.
19	LINK [transport name] SUBMIT OF MCP AS [file name] IN [library name] ON [volume name] FAILED, RETURN CODE = [SUBMIT SVC Return Code]

nn	Meaning
20	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] CICS LOGOFF ISSUED The CICS logoff was issued (as defined in WSNEDIT). This does not mean that the logoff was successful. It means that the logoff was issued.
21	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] CICS LOGON ISSUED
22	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] 2ND SIGNON ISSUED The second sign-on required by CICS (for security purposes) was issued by the VS. The sign-on is configured with WSNEDIT.
23	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] CICS LOGON(S) FAILED. CHECK CICS, LINE, AND DEVICE CONFIGURATION. LAST MESSAGE FROM HOST = [message text]
24	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] CICS LOGON(S) SUCCESSFUL
25	LINK [transport name] VALUE OF [#] NOT IN VALID RANGE. NEW VALUE = [#] One of the timeout values specified in WSNEDIT (Manage Transports) for the IDS transport was not in the proper range. Prior to WSN VS NETCORE Release 8.31, WSNEDIT did not perform checks against timeout values.
26	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] CICS SESSION FAILURE. LAST MSG FROM HOST = [message text] This message may be logged during the logoff process. It does not indicate a session failure, but is simply an indication that an SSCP-LU session is in progress.
27	LINK [transport name] DEVICE [LU # as defined in SNAEDIT] CONFIG FILE ERROR, PU NAME = [PU name as defined in SNAEDIT]

GML Link Driver Log Messages (WSN06)

GML Link Driver log messages are presented in the form WSN06nn (where nn reflects the number of the specific message expressed in decimal form).

nn	Meaning
01	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS PENDING ENABLE
02	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS ENABLED
03	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS PENDING DISABLE
04	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS DISABLED
05	802.3 TRANSPORT ON SYSTEM [system name] ENABLE FAILED
06	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS UNABLE TO TRANSMIT DATA. REASON = [#/description] For possible reason values, see the section entitled "GML Link Driver Reason Codes."
10	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] RETURNED UNDELIVERABLE DATA. REASON = [#/description] For possible reason values, see the section entitled "GML Link Driver Reason Codes."
11	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] RECEIVED ERROR ON I/O COMPLETION
12	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS ATTEMPTING RESTART. REASON = [#/description] Microcode is being reloaded following a DLP crash. For possible reason values, see the section entitled "GML Link Driver Reason Codes."

nn	Meaning
13	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] IS PENDING RESTART Microcode is pending reload following a DLP crash.
14	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] HAS BEEN RESTARTED Microcode has been reloaded following a DLP crash.
15	802.3 TRANSPORT LINK [transport name] ON SYSTEM [system name] HAS FAILED TO RESTART An attempt to reload microcode following a DLP crash has failed. The reload of microcode is attempted once every minute for 10 minutes, then once every 15 minutes indefinitely or until reload is successful.

REASON CODES AND TRANSPORT DIRECTIONS

The following are lists of SubTask Scheduler (STS) reason codes, End-to-End layer reason codes, Switching layer reason codes, transport driver reason codes, IDS reason codes, GML link driver reason codes, and transport driver directions.

Subtask Scheduler (STS) Reason Codes

The following is a list of SubTask Scheduler reason codes:

Reason Code		
Hex	**Decimal**	**Meaning**
00	00	NORMAL COMPLETION
01	01	UNKNOWN SUBTASK ID Internal code/OS error.
02	02	MAXIMUM CHECK ELEMENTS EXCEEDED Internal code/OS error.

Reason Code		
Hex	**Decimal**	**Meaning**
03	03	SUBTASK PUT XMIT ERROR Unable to send an ITM through the operating system.
04	04	BUFFER FREED TWICE Internal code/OS error.
05	05	STS STACK OVERFLOW Internal code/OS error.
06	06	GETMEM ERROR IN CREATEP Unable to create the ITM port due to insufficient memory space.
07	07	GETHEAP ERROR IN MALLOC Internal code/OS error.
08	08	GETHEAP ERROR IN STDBALOC Internal code/OS error.
30	48	CNS PROGRAM CHECK Internal code/OS error.
31	49	CNS CANCELLED BY OPERATOR
32	50	NETPORT OPEN ERROR Another CNS task is running on the system.
33	51	NETPORT RESPONSE XMIT ERROR Internal code/OS error.

Reason Code Hex	Decimal	Meaning
34	52	MCP ERROR Internal code/OS error.
35	53	EENM UNRECOGNIZED COMMAND Internal code/OS error.
36	54	NMEE UNRECOGNIZED COMMAND Internal code/OS error.
37	55	CONFIG OPEN ERROR Could not open the system CONFIG file. The file may be corrupted.
38	56	CONFIG CLOSE ERROR Problem encountered with system CONFIG file. Check the file/volume for possible disk problems.
39	57	CONFIG RECORD NOT FOUND The system CONFIG file may be corrupted. Check the file/volume for possible disk problems.
3A	58	ALTERNATE INDEX FUNCTIONS NOT SUPPORTED Internal code/OS error.
3B	59	CONFIG READ ERROR A problem was encountered with system CONFIG file. Check the file/volume for possible disk problems.
3C	60	EENM UNRECOGNIZED PROTOCOL Internal code/OS error.

Reason Code Hex	Reason Code Decimal	Meaning
46	70	SWNM UNRECOGNIZED COMMAND Internal code/OS error.
47	71	SWNM LINK TABLE MAXIMUM EXCEEDED Internal code/OS error.
48	72	SWNM UNKNOWN LINK DRIVER Internal code/OS error.
49	73	SWEE INVALID SYSTEM ID Internal code/OS error.
4A	74	SWEE UNRECOGNIZED COMMAND Internal code/OS error.
4B	75	SWEE INACTIVE LINK Internal code/OS error.
4C	76	SWLD UNRECOGNIZED COMMAND Internal code/OS error.
4D	77	SWLD UNRECOGNIZED TYPE Internal code/OS error.
50	80	INVALID FRAGMENT Internal code/OS error.
51	81	PROGERR Internal code/OS error.

Reason Code Hex	Reason Code Decimal	Meaning
52	82	CCF INVALID REQUEST TYPE Internal code/OS error.

End-to-End Layer Reason Codes

The following is a list of End-to-End layer reason codes. These messages can appear (in hex) in NTUs and (in decimal) in CNS Manager log messages.

Reason Code Hex	Reason Code Decimal	Meaning
00	00	APPLICATION GENERATED The application rejected an incoming session request.
02	02	REMOTE APPLICATION NOT ATTACHED Use the CNS Manager to check the application status on the remote system. If the application is not attached, submit the application. If the application is listed as attached, the session limit for the application was probably reached; wait for a session to complete.
06	06	SESSION LIMIT EXCEEDED AT REMOTE SYSTEM
07	07	SESSION ESTABLISHMENT INHIBITED BY REMOTE SYSTEM
09	09	INSUFFICIENT (system or CNS) RESOURCES AT REMOTE SYSTEM
0A	10	APPLICATION LOST The application terminated abnormally. Check the Operator's Console for messages. Check the print queue for dump files; dump files may indicate the reason. Resubmit the application.
0B	11	SESSION TERMINATED BY REMOTE OPERATOR

Reason Code Hex	Reason Code Decimal	Meaning
0C	12	PROTOCOL VIOLATION The command received by the End-to-End layer was unintelligible.
0D	13	RETRANSMISSION LIMIT EXCEEDED
0E	14	REMOTE SYSTEM RESTARTED There was a forced restart on the remote system; WSNSTART was run on the remote system.
0F	15	END-TO-END LAYER REVISION LEVEL UNACCEPTABLE The End-to-End layer revision levels that were exchanged during restart did not match. Use the CNS Manager to check the CNS revision levels. CNS may require restarting on both systems.
11	17	REMOTE SYSTEM NOT REACHABLE Use the CNS Manager Event Inquiry Facility to check the log for Switching layer and Transport layer messages, and for possible reasons for the failure.
12	18	CONNECTION TIMEOUT The DLP timed out before data transfer.
16	22	SESSION LIMIT EXCEEDED ON LOCAL SYSTEM
17	23	SESSION ESTABLISHMENT INHIBITED BY LOCAL SYSTEM
19	25	INSUFFICIENT (system or CNS) RESOURCES ON LOCAL SYSTEM
1B	27	SESSION TERMINATED BY LOCAL OPERATOR

Reason Code Hex	Reason Code Decimal	Meaning
1C	28	INCOMPATIBLE PRESENTATION LAYERS The (Presentation layer) NAI revision levels are incompatible on the source and destination systems.

Switching Layer Reason Codes

The following is a list of the Switching layer reason codes. The messages can appear (in hex) in NTUs and (in decimal) in CNS Manager log messages.

Reason Code Hex	Reason Code Decimal	Meaning
00	00	NO REASON Indicates a normal close/completion with no problems.
01	01	INVALID WANGNET REVISION LEVEL IN (Transport Layer) XID EXCHANGE The WangNet revision levels that were exchanged between the Transport layers on the local and adjacent systems are not compatible.
02	02	INVALID SOURCE SYSTEM ID IN (Transport Layer) XID EXCHANGE The local system names exchanged between the Transport layers on the local and adjacent system are not compatible.
03	03	INVALID DESTINATION SYSTEM ID IN (Transport Layer) XID EXCHANGE The remote system names exchanged between the Transport layers on the local and adjacent system are not compatible.

Reason Code Hex	Reason Code Decimal	Meaning
04	04	ZERO HOP COUNT The NTU being transferred has exceeded the limit of six hops (or five intermediate systems) between the source and destination systems.
05	05	INVALID SUBTASK SCHEDULER ID Internal code error.
06	06	UNKNOWN SENDER The sending system is not listed in the receiving system's Network Directory file.
07	07	INVALID XID LEVEL The Switching layer revision levels on the local and adjacent systems are not compatible.
08	08	INACTIVE ROUTE The link (transport) may be disabled or blocked.
09	09	UNDELIVERABLE MESSAGE RECEIVED
0A	10	PATH REJECT
0B	11	NO ALTERNATE ROUTE There is no alternate transport for the selected path (next hop).
0C	12	INVALID SYSTEM ID The destination System ID is not listed in the local Network Directory file.
0D	13	SWITCHING LAYER XID'S NOT EXCHANGED

Reason Code Hex	Decimal	Meaning
0E	14	INACTIVE LINK The link is either disabled or blocked.
0F	15	DESTINATION SYSTEM RESTARTED CNS on the remote system was restarted; WSNSTART was run.
10	16	INVALID COMMAND Internal code error.
11	17	NO ACTIVE PATH There is no next-hop system with an enabled, nonblocked link to the destination system.
12	18	TABLE SIZE ERROR Internal code error.
13	19	INVALID LINK ID Internal code error.
15	21	NO AVAILABLE ROUTE There is no available transport to the selected next-hop system.
17	23	UNDELIVERABLE XID RECEIVED The Switching layers on the local and adjacent systems are unable to successfully exchange (Switching layer) XIDs.

Reason Code Hex	Decimal	Meaning
18	24	FEATURE NOT SUPPORTED An NTU containing a Route Confirmation Control SPU was forwarded to a next-hop system running CNS Release 2.xx.xx.
19	25	ROUTE BY NAME ERROR A CNS (VS) system received an NTU containing a Write Extended SPU from a Wang PC and is unable to convert the destination system name (specified in the NTU) to an Area ID/System ID address.
1A	26	SYSTEM NOT FOUND A CNS (VS) system received an NTU containing a Write Extended SPU from a Wang PC and is unable to locate the destination system name (specified in the NTU) in the local network COMFIG file.
1B	27	OPEN ERROR A CNS (VS) system received an NTU containing a Write Extended SPU from a Wang PC and is unable to open the local network COMFIG file in order to convert the destination system name (specified in the NTU) to an Area ID/System ID address.
1C	28	READ ERROR A CNS (VS) system received an NTU containing a Write Extended SPU from a Wang PC and is unable to read the local network COMFIG file in order to convert the destination system name (specified in the NTU) to an Area ID/System ID address.
1D	29	INVALID INPUT REQUEST A software error occurred in the Switching layer code while processing an NTU containing a Write Extended SPU.
1E	30	TRANSPORT DISABLED

Reason Code Hex	Decimal	Meaning
1F	31	NO AVAILABLE PATH There is no available next-hop system to the destination system.
20	32	ACTIVE LINK DOWN
21	33	DLP ERROR The DLP had a problem executing a command from the Switching layer. The error is returned to the Switching layer by the GML (Generic Message layer) Link Driver.
22	34	GML ERROR The GML (Generic Message layer) had a problem executing a command from the Switching layer. The error is returned to the Switching layer by the GML Link Driver.

Transport Driver Reason Codes

The following is a list of the transport driver reason codes. The messages can appear (in hex) in NTUs and (in decimal) in the CNS Manager log messages.

Reason Code Hex	Decimal	Meaning
00	00	ACCEPTED
01	01	REMOTE TC PATH OPEN ERROR Unable to open a data path on the remote system.
02	02	REMOTE LINK IS DISABLED
03	03	ALL REMOTE VIRTUAL CIRCUITS ARE IN USE
04	04	INVALID LOCAL VS DEVICE NUMBER

Reason Code Hex	Reason Code Decimal	Meaning
05	05	LOCAL DLP NOT RUNNING
06	06	ALL LOCAL VIRTUAL CIRCUITS ARE IN USE
07	07	LOCAL DLP HAS NOT RESPONDED
08	08	TRANSPORTATION ERROR This message is associated with DLP-related problems (hardware and software). Contact your Wang customer representative.
09	09	RECEIVED INVALID PACKET The transport driver header in the received NTU was garbled.
0A	10	COMMUNICATIONS LOST WITH REMOTE DLP Possible causes include a break in the line, a power loss, etc.
0B	11	ACCEPT RECEIVED WHILE ERROR PENDING The transport driver received a request that it could not process; the transport driver was busy processing an error code. The transport driver recovers from this condition.
0C	12	DATA RECEIVED IN RESPONSE TO CALL The transport driver received user data in response to a Call request. The transport driver recovers from this condition.
0D	13	ACCEPT/CLEAR RECEIVED WHILE DATA TRANSFERRING Internal CNS code error.

Reason Code Hex	Reason Code Decimal	Meaning
0E	14	DATA RECEIVED AFTER CLEAR REQUEST Internal CNS code error.
0F	15	CALL REQUEST TIMED OUT Internal CNS code error.
10	16	CLEAR REQUEST TIMED OUT Internal CNS code error.
11	17	PACKET LAYER TIMEOUT Internal CNS code error.
12	18	INVALID PACKET NUMBER RECEIVED IN Ns COUNT A problem exists in the line or in the data communication equipment (DCE).
13	19	INVALID PACKET NUMBER RECEIVED IN Nr COUNT A problem exists in the line or in the data communication equipment (DCE).
14	20	INVALID INTERRUPT Internal CNS code error.
15	21	LINK FAILURE, NO RESPONSE FROM REMOTE DLP Check the line, modems, etc.

Reason Code Hex	Reason Code Decimal	Meaning
16	22	SESSION MANAGER TERMINATE REQUEST With @SESMGR@ Release 7.20 or later, @SESMGR@ issues a Terminate Session SMXM ITM to a task when a Deactivate UIOSW is received from the DLP over the control path. @SESMGR@ also issues a Terminate Session SMXM ITM to all tasks with active sessions on a link when the DLP crashes or is cleared/powered on. @SESMGR@ or the server task receives an Error Completion IOSW from the DLP, an outbound call request for the link times out, or @SESMGR@ waits for more than 1 minute for a response from the DLP to any IOCW.
17	23	DLP REQUEST The transport driver cannot interpret the IOSW sent from the DLP after the connection is lost. The IOSW is displayed.
18	24	DLP CRASH The DLP crashed with an IOSW. The IOSW is displayed.
19	25	LOCAL DLP DEVICE I/O ERROR CNS received a bad return code from the TRANSMIT, RECEIVE, or CLOSE macro. The Cause and Diagnostic codes are displayed. Contact your Wang customer representative for more information.
1B	27	CONFIGURATION ERROR There was a problem accessing the system CONFIG file.

Reason Code Hex	Decimal	Meaning
1C	28	SESSION MANAGER REJECT This message appears when the local @SESMGR@ responds to an Outbound Call Request with an Outbound Session Establishment ACK SMXM ITM containing a negative acknowledgment of something other than hex 01, 02, 0B, F1, F2, F3, or F4. The Diagnostic code which accompanies the message is the value of the negative acknowledgment rather than a (DLP-related) Diagnostic code. When the negative acknowledgment is hex 01, 02, 0B, F1, F2, F3, or F4, the message accompanying a reason code of hex 1C (decimal 28) is as follows: **Hex Message** 01 REMOTE SERVER CANNOT OPEN A TC PATH 02 REMOTE SERVER IS NOT READY 0B NODE SERVICE NOT ACTIVE F1 INVALID (OUTBOUND) VS DEVICE NUMBER F2 (OUTBOUND) DLP NOT RUNNING F3 ALL VIRTUAL CIRCUITS ARE BUSY F4 LOCAL DLP TIMEOUT
1D	29	DLP POWERED OFF
1E	30	DLP MICROCODE ERROR Possible memory parity error or a memory address error in the DLP. Press CLEAR on the DLP to force a reload of the microcode.
1F	31	INVALID WANGNET DRIVER STATE The CNS WangNet link driver received a WRITE while terminating.
20	32	DLP HAS NOT RESPONDED TO DEACTIVATION The transport driver issued a DEACTIVATE command to the DLP to bring down the virtual circuit, and the DLP did not respond.

Reason Code Hex	Reason Code Decimal	Meaning
21	33	OUTCALL TIMER EXPIRED The transport driver sent an Outbound Call Request to @SESMGR@, and there was no response within the 15-minute timeout period.
22	34	WAITING FOR PREVIOUS OUTCALL RESPONSE Another outbound Call request came in while the transport driver was waiting for @SESMGR@ to respond to a previous outbound Call request. The transport driver does not process a second outbound Call request when one is already pending.
23	35	LOCAL DLP NOT RESPONDING (PNA) The DLP responded to a previously issued IOCW with a PNA IOSW and has failed to clear the PNA within 5 minutes.
24	36	PREVIOUS ACTIVE LINE, ESTABLISHMENT FAILED The DLP is up but a connection cannot be established. Check for other messages with the Event Inquiry Facility, and check the state of the DLP and the modems.
25	37	LINE ESTABLISHMENT FAILED Check the modem, line, and so forth, and verify that the phone number configured for the ACU is correct.
26	38	LOCAL SWITCHED LINE ALREADY CONNECTED The transport may be shared by more than one system. Wait and retry.
27	39	LEASED LINE IS NOT UP Check the modem for carrier and other appropriate signals.

Reason Code Hex	Decimal	Meaning
28	40	SYSTEM NAME IS NOT IN DLP TABLES Use the WSNEDIT utility or the WSN Configuration Reporter to verify the contents of the network COMFIG file.
29	41	ERROR COMPLETION FROM DLP An IOSW/UIOSW was received from the DLP with an Error Status byte (byte 1 counting from 0) not equal to hex 00.
2A	42	LINE IS CLOSE PENDING The transport driver is bringing down the connection, or it has abnormally brought down the connection.
2B	43	SWITCHED LINE, INCOMING CALLS ONLY The point-to-point dial-up connection is configured for incoming calls only.
2C	44	CLOSE REQUESTED (DIAL TIMER) The Manual Dial Timer on a point-to-point line has expired.
2D	45	RECOVERY TIMEOUT The original initiator failed to reestablish the link in a given time period after a link was brought up; a virtual circuit was established and the link went down.
2E	46	LOCAL DEVICE OPEN FAILED A data path could not be opened with the local DLP. A return code is displayed in the CNS Manager log message.

Reason Code		
Hex	**Decimal**	**Meaning**
2F	47	UNKNOWN SYSTEM NAME
30	48	DLP CURRENTLY IN USE
31	49	NO CNS SYSTEMS ON LINK
32	50	CREATE PORT FAILED CNS was unable to create a necessary ITM port for communication with another task.
33	51	XMIT TO SESSION MANAGER FAILED Transmit of an intertask message to @SESMGR@ failed.
34	52	REMOTE CALL REQUEST IN PROGRESS
35	53	LOCAL DLP DEVICE UNAVAILABLE
36	54	REMOTE DLP PNA TIMER EXPIRED

Transport Driver Directions

The following is a list of transport driver direction codes. The codes appear in the CNS Manager log messages.

Code	Meaning
01	INBOUND
02	OUTBOUND

IDS Reason Codes

The following is a list of the IDS reason codes. The codes appear (in hex) in NTUs and (in decimal) in the CNS Manager log messages.

Reason Code Hex	Reason Code Decimal	Meaning
00	00	LINK DISABLED BY USER Look for a WSN01xx message to determine the issuer.
01	01	LU (DEVICE) IN USE One of the two LUs/devices configured for IDS is in use.
02	02	CONFIGURATION FILE ERROR An error was found when MCP accessed the MCP configuration file. Check for an error in the PU name specification.
03	03	MCP RELEASE IS PRIOR TO 2.50.00 The SNA software is a release that does not support the IDS transport.
04	04	LU (DEVICE) NOT AVAILABLE OR NOT CONFIGURED The LU/device configured in WSNEDIT for IDS use is not available according to the MCP configuration file. Check the configuration files, and also verify that the LU is being activated by the host.
05	05	CONTROLLER OFFLINE OR LU INACTIVE The TC line to the host is down.
06	06	SESSION NOT ACTIVE CNS made a request for a particular SSCP-LU or LU-LU session that is no longer active.

Reason Code Hex	Reason Code Decimal	Meaning
07	07	KEYBOARD LOCKED
08	08	NEW DEVICE STATUS INVALID
09	09	LU (DEVICE) NOT ATTACHED
0A	10	INVALID REQUEST CODE
0B	11	MCP IS NOT EXECUTING Check the procedure, background task availability, or any dumps.
0C	12	MCP HAS NO AVAILABLE BUFFERS CNS tried to send to the MCP but the MCP port is full.
0D	13	INVALID PU (or CUA) NAME
0E	14	INVALID LU (or DEVICE)
0F	15	MCP MESSAGE PENDING MCP rejected a CNS request because MCP has a message for CNS.
10	16	INVALID DATA LENGTH The CNS request to MCP has an invalid data length.
11	17	INVALID BUFFER SEQUENCE FIELD
12	18	NO MCP MESSAGE PENDING
13	19	TIMER VALUE INVALID

Reason codes hex 14 (decimal 20) to hex 1F (decimal 31) are returned to CNS by MCP. Check the SNA log and the host log for additional details.

Reason Code Hex	Reason Code Decimal	Meaning
14	20	ACTIVATION LEVEL TOO LOW, CICS DOWN
15	21	DIRECTION CONFLICT
16	22	NO SESSION SELECTED
17	23	TRANSFER IN PROGRESS
18	24	NEGATIVE RESPONSE FROM HOST
19	25	ACTIVATION LEVEL DROP. CICS DOWN?
1A	26	SEQUENCE ERROR
1B	27	CANCEL RECEIVED
1C	28	INVALID RESPONSE CODE RECEIVED
1D	29	LU-W NOT SUPPORTED BY MCP
1E	30	SESSION SYNCHRONIZATION ERROR -- CICS DOWN?
1F	31	ALREADY ATTACHED
20	32	DEVICE NOT 3270 DISPLAY, CHECK DUA The Send/Receive device specified in SNAEDIT is not genned as a 3270 Display Terminal. Check the configuration on the VS and on the host.

Reason Code Hex	Decimal	Meaning
21	33	NULL TRANSACTION RECEIVED, CICS DOWN? CNS received a null transaction of 00.
22	34	CNS-MCP PROTOCOL SEQUENCE ERROR
23	35	SIGNON COMMAND ISSUED IN INVALID STATE CNS received a SIGN-ON command from the host, but CNS is in an invalid state for a SIGN-ON.
24	36	HOST OR MCP TIMEOUT. NO RESPONSE RECEIVED.
25	37	INVALID COMMAND The IDS transport driver received an invalid command from the CNS Switching layer.
26	38	ATTACH RETRY EXHAUSTED
27	39	SIGNON RETRY EXHAUSTED
28	40	SIGNOFF RETRY EXHAUSTED

Reason codes hex 29 (decimal 41) to hex 32 (decimal 50) are returned to CNS by the (host) IDS application. These codes should not be confused with the SNA negative response codes and sense codes as defined by IBM.

Reason Code Hex	Decimal	Meaning
29	41	HOST-RSP: IDS NOT ACTIVE
2A	42	HOST-RSP: LINK IS DISABLING
2B	43	HOST-RSP: INVALID STATE FOR SIGNON

Reason Code Hex	Decimal	Meaning
2C	44	HOST-RSP: INVALID REVISION NUMBER
2D	45	HOST-RSP: LINK IS ENABLING
2E	46	HOST-RSP: INVALID STATE FOR SIGNOFF
2F	47	HOST-RSP: LINK IS NOT ENABLED
30	48	HOST-RSP: DATA LOST, CHAIN ERROR
31	49	HOST-RSP: NO DATA IN DATA MESSAGE
32	50	HOST-RSP: INVALID SUBNET CLASS

Reason codes hex 34 (decimal 52) to hex 3C (decimal 60) are returned to the (host) IDS application by CNS.

Reason Code Hex	Decimal	Meaning
34	52	VS-RSP: LINK IS DISABLING
35	53	VS-RSP: INVALID STATE FOR SIGNON
36	54	VS-RSP: INVALID REVISION NUMBER
37	55	VS-RSP: LINK IS ENABLING
38	56	VS-RSP: INVALID STATE FOR SIGNOFF
39	57	VS-RSP: LINK IS NOT ENABLED
3A	58	VS-RSP: DATA LOST, CHAIN ERROR
3B	59	VS-RSP: NO DATA IN DATA MESSAGE

Reason Code Hex	Decimal	Meaning
3C	60	VS-RSP: INVALID SUBNET CLASS
3D	61	HOST INITIATED SIGNOFF
3E	62	VS INITIATED SIGNOFF
3F	63	HOST INITIATED SIGNOFF RETRY
40	64	HOST SIGNOFF, IDS SHUTDOWN

In reason codes hex 43 (decimal 67) to hex 47 (decimal 71), the CNS-sending LU/device sent a protocol violation to the host for the stated reason. Examine the SNA log and the host log for additional information.

Reason Code Hex	Decimal	Meaning
43	67	S SENT PV: INVALID HEADER LENGTH
44	68	S SENT PV: LINK DISABLED
45	69	S SENT PV: INVALID HEADER TYPE
46	70	S SENT PV: RESPONSE RECEIVED IN INVALID STATE
47	71	S SENT PV: CATCH ALL

In reason codes hex 4A (decimal 74) to hex 4F (decimal 79), the CNS-sending LU/device received a protocol violation from the host for the stated reason. Examine the SNA log and the host log for additional information.

Reason Code Hex	Decimal	Meaning
4A	74	S RCVD PV: INVALID HEADER LENGTH

Reason Code Hex	Decimal	Meaning
4B	75	S RCVD PV: LINK DISABLED
4C	76	S RCVD PV: INVALID HEADER TYPE
4D	77	S RCVD PV: RESPONSE RECEIVED IN INVALID STATE
4E	78	S RCVD PV: INVALID TERMINAL ID
4F	79	S RCVD PV: CATCH ALL

In reason codes hex 52 (decimal 82) to hex 58 (decimal 88), the CNS-receiving LU/device sent a protocol violation to the host for the stated reason. Examine the SNA log and the host log for additional information.

Reason Code Hex	Decimal	Meaning
52	82	R SENT PV: INVALID HEADER LENGTH
53	83	R SENT PV: LINK DISABLED
54	84	R SENT PV: INVALID HEADER TYPE
55	85	R SENT PV: RESPONSE RECEIVED IN INVALID STATE
56	86	R SENT PV: ENCODE BYTE INVALID
57	87	R SENT PV: INVALID SIGNOFF RETURN CODE
58	88	R SENT PV: CATCH ALL

In reason codes hex 5B (decimal 91) to hex 60 (decimal 96), the CNS-receiving LU/device received a protocol violation from the host for the stated reason. Examine the SNA log and the host log for additional information.

Reason Code Hex	Decimal	Meaning
5B	91	R RCVD PV: INVALID HEADER LENGTH
5C	92	R RCVD PV: LINK DISABLED
5D	93	R RCVD PV: INVALID HEADER TYPE
5E	94	R RCVD PV: RESPONSE RECEIVED IN INVALID STATE
5F	95	R RCVD PV: INVALID TERMINAL ID
60	96	R RCVD PV: CATCH ALL
62	98	WRITE UNDELIVERABLE - LINK IS NOT ENABLED
63	99	WRITE UNDELIVERABLE - LINK IS DISABLING
64	100	IDS DRIVER NOT ON SYSTEM Reinstall the software.
65	101	CATCH ALL - NEGATIVE RESPONSE SENT
66	102	CATCH ALL - NEGATIVE RESPONSE RECEIVED

GML Link Driver Reason Codes

The following is a list of the GML link driver reason codes. The codes appear (in hex) in NTUs and (in decimal) in the CNS Manager log messages.

Reason Code Hex	Decimal	Meaning
00	00	NO REASON
01	01	CONFIGURATION ERROR There is a problem accessing the network directory file. Use the WSNEDIT utility to verify that the file can be opened/read.

Reason Code Hex	Reason Code Decimal	Meaning
02	02	NO LSAP IN CONFIGURATION RECORDS There is no Link Service Access Point (LSAP) address in the network directory file for the LAN system being addressed.
03	03	SYSTEM NOT IN NAME TABLE The LAN system addressed is not in the dynamic internal microcode name table.
04	04	LSAP TABLE FULL Microcode has no additional buffer space for the inclusion of another Link Service Access Point (LSAP) address.
05	05	INVALID LSAP ADDRESS Data was addressed to a system (LSAP address) on the LAN; the system is not configured in the (local microcode) LSAP table. Each active system on the LAN periodically broadcasts its LSAP across the LAN. The LSAP is detected by the VS microcode and is dynamically added to the LSAP table, provided it does not already exist in the table. The LSAP on a remote system is also periodically deleted from the LSAP table by the VS microcode if, within so many seconds, no data of any kind (including the periodically broadcast remote LSAP) has been received from the remote.
06	06	LSAP PREVIOUSLY DEFINED An attempt was made to enable a link, and two or more systems are configured with the same Link Service Access Point (LSAP) address. In WSN VS NETCORE Release 8.32, LSAPs are hardcoded and are not configurable or modifiable. PC LSAPs are configurable with the SCPARMS program.

Reason Code Hex	Reason Code Decimal	Meaning
07	07	LSAP NOT CURRENTLY ACTIVE The link is not enabled.
08	08	ADD LSAP ERROR An error condition was encountered during link enable. The attempt by the microcode to add a Link Service Access Point (LSAP) address to the internal tables was unsuccessful.
09	09	INITIALIZATION ERROR GML cannot be properly initialized during a link enable.
0A	10	OPEN ERROR GML cannot be properly opened during a link enable.
0B	11	CONNECT ERROR GML cannot be properly connected during a link enable.
0C	12	LAN CONTROLLER ERROR The message indicates a hardware-related problem.
0D	13	802.3 CONTROLLER HAS NO BUFFERS The microcode has no buffers for data transfer.
0E	14	MEDIA TRANSMISSION FAILURE The message indicates a cable-related hardware problem.

Reason Code Hex	Decimal	Meaning
0F	15	DESTINATION NOT ACTIVE ON LAN There is no Link Service Access Point (LSAP) address configured on the LAN for the destination system. Each active system on the LAN periodically broadcasts its LSAP across the LAN. The LSAP is detected by the VS microcode and is dynamically added to the LSAP table, provided it does not already exist in the table. The LSAP on a remote system is also periodically deleted from the LSAP table by the VS microcode if, within so many seconds, no data of any kind (including the periodically broadcast remote LSAP) has been received from the remote.
10	16	802.3 CONTROLLER FAILURE There is a hardware failure involving an 802.3 controller card.
11	17	TRANSPORT RESET Microcode reload is being attempted following a DLP crash.
12	18	SESSION MANAGER ERROR A problem was encountered while setting up a link and attempting to connect to GML.

DLP CODES

The following lists the DLP codes that are currently defined.

Hex Code	Description
0000	UNEXPECTED INTERRUPT FROM SIO CHANNEL 0
0001	UNEXPECTED INTERRUPT FROM SIO CHANNEL 1
0002	UNEXPECTED INTERRUPT FROM SIO CHANNEL 2
0003	UNEXPECTED INTERRUPT FROM SIO CHANNEL 3
0004	UNEXPECTED INTERRUPT FROM SIO CHANNEL 4
0005	UNEXPECTED INTERRUPT FROM SIO CHANNEL 5
0006	UNEXPECTED INTERRUPT FROM SIO CHANNEL 6
0007	UNEXPECTED INTERRUPT FROM SIO CHANNEL 7
0008	UNEXPECTED INTERRUPT FROM CTC CHANNEL 0

Hex Code	Description
0009	UNEXPECTED INTERRUPT FROM CTC CHANNEL 1
000A	UNEXPECTED INTERRUPT FROM CTC CHANNEL 2
000B	UNEXPECTED INTERRUPT FROM CTC CHANNEL 3
000C	NON-MASKABLE INTERRUPT/DEADMAN TIMER EXPIRED
000D	MASTER MONITOR OVERFLOW INTERRUPT
000E	INVALID VECTORED INTERRUPT
000F	INTERRUPTS FOUND DISABLED BY DISPATCHER
0010	OSBUFGTI FOUND BUFFER POOL EMPTY
0011	OSBUFGTN FOUND BUFFER POOL EMPTY
0012	INVALID BUFFER NUMBER PASSED IN SUBROUTINE CALL
0013	BUFFER TO BE RELEASED/CHAINED IS STAMPED FREE
0014	BUFFER CONTROL TABLE CORRUPTED
0015	RELEASED TOO MANY BUFFERS
0018	OSQUEPTI FOUND INTERRUPTS ENABLED
0019	NOT ENOUGH BUFFERS IN BUFFER CHAIN
001A	TOO MANY BUFFERS IN BUFFER CHAIN
001B	QUEUE COUNT OVERFLOW (MORE THAN 127 ENTRIES)
001C	INVALID QUEUE ENTRY SIZE
0020	INVALID TIMER EXPIRATION TYPE
0021	INVALID TIMER RB TYPE
0028	INVALID CALL FOR NON-SUSPENDABLE TASK
0029	INVALID STATE IN TCB
002A	TASK STARTED FROM INTERRUPT LEVEL DOES NOT RUN ON OSQUEUE0
002B	TASK TO BE READIED WAS NOT SUSPENDED
002C	ATTEMPT TO SIGNAL WITH EVENT CODE = 0
002D	ATTEMPT TO SIGNAL/WAIT WITH TCB ADDRESS = 0
002E	INVALID REQUEST RETURN TYPE PASSED TO OS$REQST OR OS$REPLY
002F	SUSPENDABLE TASK PRIMITIVES NOT CONFIGURED
0030	BUFFER TABLE NOT LINKED ON PAGE BOUNDARY
0033	NO MORE SLOTS LEFT IN INTERRUPT VECTOR TABLE
0034	MASTER OR DATA LINK MONITOR ADDRESS OUTSIDE VALID RANGE
0038	LCB ADDRESS BELOW HEX 0100
0039	LIST ELEMENT ADDRESS BELOW HEX 0100
003A	ELEMENT TO BE ADDED IS ALREADY ON THE LIST
0040	INVALID TASK ADDRESS FOR TASK DISPATCH
0041	TOO MANY PARAMETERS FOR TASK DISPATCH
0042	INVALID TASK QUEUE INDEX FOR OSDSPPST

Hex Code	Description
0048	ATTEMPT TO COPY DATA TO ADDRESS BELOW HEX 0100
0050	INVALID SCA COMPLETION INTERRUPT
0051	INVALID RCB COMPLETION INTERRUPT
0052	INVALID PARAMETER PASSED TO MRH$QUE
0053	INTERNAL DATA STRUCTURE ERROR
0058	ILLEGAL PRIORITY PARAMETER TO OIS FILIO
0059	ILLEGAL CONTROL PARAMETER TO OIS FILIO
005A	ILLEGAL FUNCTION CODE TO OIS FILIO READ/WRITE
0060	MCA MANAGEMENT RECEIVED INVALID REQUEST TYPE
0061	INVALID SYSTEM ID
0062	ERROR IN POSTING RESPONSE TO MASTER
0063	INVALID SLAVE RESPONSE CODE
0064	FAN TO BE RELEASED NOT IN USE
0065	MASTER ACKNOWLEDGED NON-EXISTING RESPONSE
0066	FAN ALLOCATION ERROR
0068	DUPLICATE SYSTEM ID
0069	SYSTEM NAME/ID TABLE FULL
006A	XFS INITIALIZATION ERROR
0070	RECORD OPEN REQUEST FAILED
0071	RECORD CATALOG REQUEST FAILED
0072	RECORD WRITE REQUEST FAILED
02FF	VIRTUAL CIRCUIT NUMBER TO POLL TOO HIGH
0400	DATA TERMINAL READY WENT OFF (hardware failure)
0401	DATA SET READY WENT OFF (hardware failure)
0402	RECEIVE INTERRUPT WITH FIFO EMPTY (hardware failure)
0403	HEADER ADDRESS NOT WORD ALIGNED
0404	DATA ADDRESS NOT WORD ALIGNED
0405	BCT POINTERS OUT-OF-SYNCH
0406	FIFO COUNT WENT NEGATIVE
0407	RECEIVE INTERRUPT, NO COMPLETION (hardware failure)
0408	TRANSMIT QUEUE EMPTY
0409	TRANSMIT TIMED OUT (hardware failure)
040A	TRANSMIT TO SELF
040B	RECEIVE DATA PORTION OF ONE WORD
0500	BUFFER MANAGEMENT OUT OF HEADER BUFFERS
0540	LINK LAYER - LINK RECEIVE STATUS ERROR
0541	LINK LAYER - NO RECEIVE DATA BUFFERS LEFT
0542	LINK LAYER - LINK TRANSMIT STATUS ERROR

Hex Code	Description
0600	PACKET LAYER - ILLEGAL STATE, ACTION PAIR IN LEVEL 1 STATE MACHINE
0601	PACKET LAYER - ILLEGAL STATE, ACTION PAIR IN LEVEL 2 STATE MACHINE
0602	PACKET LAYER - PACKET LEVEL BEING CALLED RECURSIVELY
0603	PACKET LAYER - ILLEGAL EVENT CODE FOR LEVEL 1 STATE MACHINE
0604	PACKET LAYER - ILLEGAL EVENT CODE FOR LEVEL 2 STATE MACHINE
0606	PACKET LAYER - UPPER LEVEL PASSED A BAD VCCB POINTER TO THE PACKET LEVEL
0680	TRANSPORT LAYER - NOT AN EMS COMMAND
0681	TRANSPORT LAYER - NO NEXT BUFFER IN CHAIN FOR A MESSAGE GREATER THAN ONE BUFFER LONG
0809	VTI - MSEM COMPLETE IN ILLEGAL STATE FOR ADVANCED IOP
0818	VNM - VIRTUAL CIRCUIT NUMBER IN READ DATA IOCW DOES NOT MATCH SCB
0819	VNM - INBOUND CALL ACCEPT USING CONTROL PATH
0830	VTI - TRACE BUFFER ERROR
0840	VNM - OUTBOUND CALL IOCW USING CONTROL PATH
0841	VNM - VIRTUAL CIRCUIT NUMBER IN OUTBOUND CALL RESPONSE DOES NOT MATCH SCB
0842	VNM - ATTEMPT TO USE NON-IDLE DCB (device re-use)
0843	VNM - ATTEMPT TO USE NON-IDLE SCB
8001	VTI - BAD STATE
8002	VTI - MSEM PROBLEM
8003	VTI - BAD EVENT CODE FROM IOP
8004	VTI - SSEM COMMAND WAS ZERO
8005	VTI - MSEM WAS NOT ZERO
8006	VTI - MSEM WAS HEX FF
8007	VTI - SSEM DEVICE WAS HEX FF
8008	VTI - START IO EVENT, BUT SIO RECEIVED FLAG NOT SET
8009	VTI - EVENT CODE WAS ZERO
800A	VTI - EVENT CODE LARGER THAN ALLOWED
8011	VNM - ILLEGAL COMMAND RECEIVED FROM IOP
8020	VTL - UNKNOWN EVENT
8021	VTL - DATA FOR A DEVICE WHICH CAN'T BE FOUND

Hex Code	Description
8022	VTL - UNSUPPORTED ENTRY FROM LOWER LAYER (reset, reset ack, interrupt or interrupt ack received)
8023	VTL - CONTROL PACKETS RECEIVED ON A VIRTUAL CIRCUIT WITHOUT A VS DEVICE ASSIGNED TO IT
8024	VTL - RESET REQUEST RECEIVED ON A VIRTUAL CIRCUIT WITHOUT A VS DEVICE ASSIGNED TO IT
8073	VNM - ATTEMPT TO SEND UIOSW IN INVALID VC STATE
80FD	VNM - MONITOR WRITE WITH OPTION ONE = FF
80FE	VTL - MONITOR WRITE COMMAND RECEIVED FROM VS WITH OPTION ONE = FF
80FF	VTL - BAD EVENT

APPENDIX C
OPERATOR'S CONSOLE NETWORK ERROR MESSAGES

INTRODUCTION

This appendix contains error messages that are sent to the Operator's Console of a VS system by either the File Transfer Manager (FTM) or the Session Manager. These error messages indicate that the FTM (of the local system) was unable to establish a file transfer session with a remote FTM or that a session was established but could not be completed.

In some of these messages, the name of the remote system is part of the message. In this appendix, SYSNAME indicates where the name of a remote system appears. Similarly, each message displays the time (indicated in the samples as TIME) when the system detected the error.

Each message in this appendix is followed by an explanation of its cause and a brief description of what you can do to correct the problem. Some of the messages have return codes that refer to more specific reasons for the transfer problem.

SERVICE CONNECTION ERRORS

One of the following messages may appear if your VS cannot activate the File Transfer service for a remote system.

Cannot access directory access file .....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Meaning
The directory file must correspond to the directory file specified through WSNDIRM.

Action
Run the WSNEDIT utility or the WSN Configuration Reporter to check validity of the network directory file. Run the WSNRORG procedure to reorganize the network directory file. (Return code = 21.)

Configuration Error, Connection not possible.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
This is a general message indicating that an error may exist either in your network configuration file defined through WSNEDIT or in the configuration file of the remote system.

Action
Verify that the correct microcode was loaded in the data link processor (DLP). In a non-CNS environment, if your local VS is a secondary system on a Multipoint link, the connection request may have been for another secondary system. Since secondary systems cannot communicate directly, a connection is not possible. (Return code = 8.)

Configuration Error, Data truncated due to lack of space..TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
This is a software error (internal code or operating system).

Action
Call your Wang analyst. (Return code = 4.)

Configuration Error, DLP not found in system config file..TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
A DLP for the link does not exist.

Action
Compare the DLP device name you entered through WSNEDIT in your local-view configuration file to your device configuration in the system configuration (i.e., GENEDIT) file. Determine whether or not the device name in the WSNEDIT local-view file properly reflects the port to which the DLP is connected. (Return code = 48.)

Configuration Error, Invalid function in parameter list...TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
This is a software error.

Action
Call your Wang analyst. (Return code = 28.)

Configuration Error, Invalid link or link definition.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
Invalid transport or transport definition.

Action
Use WSNEDIT or the WSN Configuration Reporter to check the definition of the transport. Check to see if the remote system is defined for that transport. (Return code = 20.)

Configuration Error, Invalid operand.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
This is a software error.

Action
Call your Wang analyst. (Return code = 32.)

Configuration Error, Invalid service or service ID.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
File Transfer was not declared as a service for the remote system.

Action
Check your WSNEDIT local-view configuration file to see if the File Transfer service is declared for the remote system. (Return code = 12.)

Configuration Error, Invalid system or system ID.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Action
Check your WSNEDIT local-view configuration file and the network directory file to see if the remote system is defined properly and to see if its network name (as defined in its configuration file) matches the name assigned to it in your configuration file and the network directory file. (Return code = 16.)

Configuration Error, Link initialization not possible.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
Transport initialization is not possible.

Action
Use GENEDIT to check your system configuration file to see if the DLP for that transport is configured properly, or use CNSMGR to see if the transport is disabled. (Return code = 40.)

Configuration Error, Link not supported.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
A link is not defined for the remote system, or the remote system is not defined in the local system's network configuration file.

Action
Use WSNEDIT or the WSN Configuration Reporter to check the configuration file.

Configuration Error, No configuration file available.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Action
Perform IPL on your system with a valid WSNEDIT configuration file. (Return code = 36.)

Configuration Error, System not configured for service....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Meaning
The File Transfer service was not specified as a service for the remote system.

Action
Check with the system administrator of the remote system. (Return code = 24.)

Configuration Error, Unknown network config file problem...TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Action
Save the network configuration file for further analysis, or print the configuration file with the WSN Configuration Reporter. Re-IPL the system using a backup configuration file, or recreate the configuration file with WSNEDIT.

DLP for SYSNAME is currently in use for other purposes ....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Meaning
All the available sessions to the remote system are active.

Action
Try to establish a session later.

File Transfer configuration error for system SYSNAME .....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Meaning
The remote system may not be defined properly in your network directory file or local-view configuration, or the File Transfer service was not declared for that system.

Action
Check your network directory file and your local-view configuration file.

FTM communication with Network Server failed .....TIME
Will try to re-attach to Network Server when its running..TIME

Meaning
This message appears under two conditions. The first condition occurs when the CNS task is not running. If CNS is not running, it must be started before FTM can use it. The second condition occurs when communication with CNS task fails during the processing of transfer requests. In either case, transfer requests should be released after CNS is re-activated. FTM will then attempt to re-attach to CNS and process the next release entries on the queue. (Return code = 07.)

Local system is not configured .....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Meaning
The local system must be defined for the File Transfer service.

Action
Run WSNEDIT (Manage Services) to check the local-view configuration file, or run the WSN Configuration Reporter. (Return code = 20.)

Network application limit exceeded .....TIME
Allow File Transfer Service to SYSNAME has failed .....TIME

Meaning
File Transfer service cannot attach to CNS because maximum number of applications that can attach to CNS has been exceeded. (Return code = 03.)

Action
Contact your network administrator.

Network Server directory file error, Data not found .....TIME
Allow File Transfer Service to SYSNAME has failed .....TIME

Action
System record cannot be found.

Meaning
Run WSNEDIT or the WSN Configuration Reporter to check the directory for the name of the system in question. If the name is not in the directory, use WSNEDIT to enter the system name. (Return code = 01.)

Network Server directory file error, File access error ...TIME
Allow File Transfer Service to SYSNAME has failed .....TIME

Meaning
An error occurred while the directory file was being read.

Action
Check the directory file to determine whether or not it requires reorganization. (Return code = 03.)

Not enough memory to create an inter-task message port ..TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Action
Check your system's memory usage. (Return code = 22.)

SESSION ESTABLISHMENT ERRORS

One of the messages in this section may appear if your VS can establish a connection with a remote system but cannot establish a File Transfer session. The VS File Transfer Manager will try to establish a session every few seconds up to a specified number of times. When the File Transfer Manager has tried for the last time, the message is displayed

Maximum session retries with SYSNAME reached ...TIME

This message is displayed in conjunction with any of the following messages:

All available circuits are busy for system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
There are no available logical circuits to the remote system.

Action
Try to establish a session later.

Communication timeout while trying to reach SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
Timer expired while waiting for a response from the remote system.

Action
Use the CNS Manager to check routes, traffic volume, and other network factors to determine the cause of the delayed response. (Reason code = 18.)

File Transfer mailbox ID not attached to network server .....TIME
File Transfer session establishment has failed .....TIME

Meaning
File Transfer has a mailbox ID that allows CNS to deliver messages to it. This ID must be attached to CNS in order for a file transfer to take place.

Action
Inhibit File Transfer and re-allow it for all systems. (Return code = 01.)

File Transfer service inhibited by system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The remote system administrator has inhibited communications.

Action
Try to establish a session later.

File Transfer session limit exceeded .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The maximum number of concurrent incoming "open session" requests sent by CNS has been reached.

Action
Check the number of active sessions. Try to establish a session later. (Return code = 04.)

FTM not active at SYSNAME or passwords do not agree .....TIME
File Transfer session establishment has failed .....TIME

Meaning
Transfers to the remote system cannot be completed.

Action
Check to determine whether or not transfers are allowed to the remote system. Use WSNEDIT (Manage Services function) or the WSN Configuration Reporter to verify that the password expected at the remote system is the one contained in the local system's local-view configuration file. (Reason code = 00.)

Insufficient resources at local system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The local system is involved in a large volume of network activity.

Action
Check the volume of activity at the local system. (Reason code = 25.)

Insufficient resources at remote system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The remote system lacks the resources required to handle a session.

Action
Check with the system administrator at the remote system about the amount of activity there. (Reason code = 09.)

Invalid system, system record not found on directory .....TIME
File Transfer session establishment has failed .....TIME

Meaning
System record for a system was not found in the directory.

Action
Use WSNEDIT or the WSN Configuration Reporter to check the directory file for the name of the system. (Return code = 02.)

Local FTM session limit at SYSNAME exceeded .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The maximum number of concurrent file transfer sessions at the local system has been exceeded.

Action
Check the number of active sessions at the local system. (Reason code = 22.)

Maximum number of File Transfer sessions for SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
All sessions to the remote system are in use.

Action
Try to establish a session later.

Password received by SYSNAME is not as configured .....TIME
File Transfer session establishment rejected by SYSNAME .....TIME

Meaning
The password that your VS sent to the remote system does not match the password that the remote system expected to receive.

Action
Check with the remote system administrator to see if your system's password (as listed in WSNEDIT) matches the Receive password listed in the remote system's network configuration file.

Remote FTM at SYSNAME could not be found .....TIME
File Transfer session establishment has failed .....TIME

Meaning
File Transfer at the remote system could not be accessed.

Action
Check the status of File Transfer at the remote system. (Reason code = 10.)

Remote FTM at SYSNAME not attached to network server .....TIME
File Transfer session establishment has failed .....TIME

Meaning
File Transfer service at the remote system is either completely inhibited or not currently attached to CNS. (Reason code = 02.)

Action
Contact the system administrator at the remote system.

Remote session limit at SYSNAME exceeded .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The maximum number of concurrent sessions at the remote system has been exceeded.

Action
Use the CNS Manager to check the number of active sessions using CNS at the remote system. (Reason code = 06.)

Remote system SYSNAME is not reachable .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The remote system could not be reached.

Action
Use the CNS Manager to check all CNS routes between the originating system and the destination system. Check for messages in the CNS Manager Event Inquiry Facility from other CNS layers. (Reason code = 17.)

Session is not active .....TIME
File Transfer session establishment has failed .....TIME

Meaning
A session that was active is no longer active. All active transfers will be placed on hold.

Action
Check transfer and retrieve queues and release items to re-initiate transfers. (Return code = 05.)

System name received from SYSNAME is not as configured .....TIME
File Transfer session establishment has failed .....TIME

Meaning
The name that the remote system uses to identify itself on the network is not the name your system expected to receive.

Action
Use WSNEDIT or the WSN Configuration Reporter to check your configuration file to see if the name you entered for that system is correct.

System SYSNAME is not available at this time .....TIME
File Transfer session establishment has failed .....TIME

Meaning
All available virtual circuits to the remote system are in use.

Action
Try to establish a session later.

System SYSNAME is unable to establish File Transfer .....TIME
File Transfer session establishment has failed .....TIME

Meaning
A problem exists at the remote system.

Action
Contact the remote system administrator.

System SYSNAME is unable to establish File Transfer Session...TIME
All virtual circuits are busy .....TIME

Meaning
The remote system is currently engaged in its maximum number of communications sessions.

Action
Try to establish a session later. (Return code = 243.)

System SYSNAME unable to establish File Transfer Session .....TIME
Cannot open a telecommunication path .....TIME

Meaning
A problem may exist with your DLP or with the DLP of the remote system.

Action
Check the system configuration files of both systems to verify the configuration of the DLPs. Check the status LEDs of the DLPs. (Return code = 01.)

System SYSNAME unable to establish File Transfer Session.....TIME
DLP has the maximum number of active sessions .....TIME

Meaning
Either the local or the remote DLP is conducting the maximum number of sessions.

Action
Try to establish a session later. (Return code = 12.)

System SYSNAME unable to establish File Transfer Session .....TIME
DLP not running (outbound) .....TIME

Meaning
Either the remote or the local DLP is not operating.

Action
Activate the DLP. (Return code = 242.)

System SYSNAME unable to establish File Transfer Session.....TIME
Invalid VS device number .....TIME

Meaning
A system cannot access a VS device (in this case a DLP).

Action
Use WSNEDIT (or WSN Configuration Reporter) and GENEDIT to see if the DLP is identified properly. (Return code = 241.)

System SYSNAME unable to establish File Transfer Session.....TIME
Local DLP timeout .....TIME

Meaning
The local DLP did not receive a response from the remote DLP in the allowed period of time. (Return code = 244.)

Action
Try to establish a session later.

System SYSNAME unable to establish File Transfer Session.....TIME
Maximum number of sessions per system has been reached .....TIME

Meaning
All guaranteed file transfer sessions to a remote system are in use.

Action
Try to establish a session later. (Return code = 49.)

System SYSNAME unable to establish File Transfer Session.....TIME
Session will shut down other system's guaranteed session .....TIME

Meaning
The session you have tried to establish has a higher priority than a current session.

Action
The other session will be canceled if you continue.
(Return code = 13.)

System SYSNAME unable to establish File Transfer Session.....TIME
System is not active .....TIME

Meaning
Either the local VS is not listed in the configuration file of the remote VS, or the File Transfer service has not been activated for the local VS by the remote VS system administrator.

Action
Call the system administrator of the remote VS. (Return code = 11.)

System SYSNAME unable to establish File Transfer Session.....TIME
Transportation error .....TIME

Meaning
Possible reasons for the appearance of this message are

Remote VS has all circuits in use.
Communications are lost.
Switched line establishment has failed.
Leased line is not up yet.
System name is not in destination table.
Line is in the process of closing.
Switched line is not up. It is configured for incoming calls only.
Close requested (manual dial timer has expired).

(Return code = 245 for any of the messages above.)

System SYSNAME unable to establish File Transfer Session.....TIME
Unable to access user list. .....TIME

Meaning
A specific user ID or password cannot be validated.

Action
You must run the SECURITY utility on the remote VS and correct the user ID error condition. (Return code = 19.)

Unable to open a TC path for system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Meaning
A problem may exist with the configuration of the DLP or with the communications line.

Action
Check your DLP, its configuration, and its status lights.

APPENDIX D
PROBLEM SOLVING

INTRODUCTION

This appendix discusses the light emitting diode (LED) status lights for Cable Interface Units (CIUs), VS Telecommunications Controllers (VS-TCs), the Multi-Line Telecommunications Controller (MLTC), and modems. LEDs indicate the operational status of their devices; you can use them to determine if there are problems with either the devices or the data link.

This appendix also covers some of the steps you might take when trying to discover the cause of a communications failure. Some of the hardware descriptions in this appendix are for your information only. Only a qualified Wang analyst should perform certain adjustments to hardware devices.

TCB LIGHT EMITTING DIODES

Figure D-1 illustrates the VS-TC (TCB1) and VS-TC1 (TCB3) light emitting diodes (LEDs) as they appear on the front panel. Reading from left to right, they are numbered 1 through 8. Table D-1 gives the meaning of each VS-TC LED.

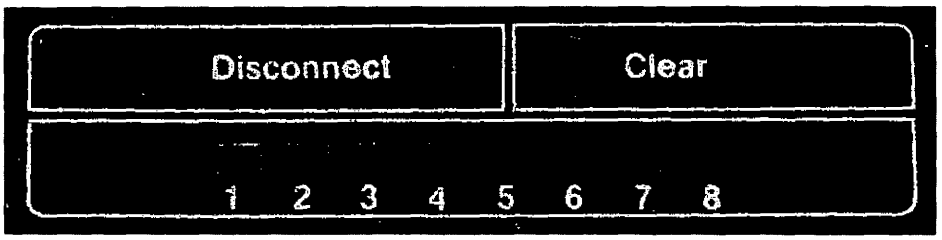

Figure D-1. VS-TC LEDs

Table D-1. VS-TC LED Meanings

LED	Indicates	Description
1	System activity	When the VS-TC is operating normally, this LED blinks several times per second to indicate that the VS-TC has been loaded successfully. If no other LEDs are lit (LED 8 should be ON), the VS-TC is waiting for a line to come up. If the LED is blinking slowly, large amounts of message traffic requiring compression are being processed.
2	Receive data	This LED indicates that the VS-TC is receiving data without transmission errors. The LED changes each time the VS-TC receives a message (it should always be blinking if operations are either polling on Multipoint or continuity checking for Point-to-Point).
3	Transmit data	When this LED is on, the VS-TC is transmitting data on the line (data, polls, continuity checking). Unlike LED 2, this LED is on only when the VS-TC is actively transmitting.
4	Data carrier	When lit, this LED indicates that both the local and remote modems are operating. It is on steadily when a full-duplex line is being used, and blinking when a half-duplex line is being used.
5	Session active	If this LED is on, at least one communications session has been established. This LED can mean, for example, that a user has logged on to a remote VS or that the File Transfer Manager is active.
6	System traffic active	When this LED is on, the TCB is exchanging information with the main memory. LEDs 2 and 3 indicate that the VS-TC is exchanging data over the link. This LED indicates that the VS-TC is exchanging data with your system.

(continued)

Table D-1. VS-TC LED Meanings (continued)

LED	Indicates	Description
7	Refusing new traffic	When this LED is on, the TCB has more traffic than it can handle and is temporarily refusing additional user messages. This is not a fatal condition, because the software has extensive logic to prevent traffic from increasing to a fatal level. If this LED is on frequently, however, performance is suffering, and you should consider more communications hardware or operation at a faster line speed.
8	Diagnostic mode	This LED should be on and not blinking during an operation. It indicates that the VS-TC is in normal operation.
	Idle mode	LEDs flashing in sequence from left to right indicate that the VS-TC is in an idle state.

If LED 1 is blinking and LED 8 is on steadily, the microcode was loaded, but a logical connection is not yet established.

If LED 8 is on steadily and the other lights are flashing in sequence from right to left, the microcode is loaded, but the session manager has not yet sent the configuration to the DLP.

EXTERNAL CABLE INTERFACE UNIT LEDs

Front Panel

The front panel of an external CIU has three LEDs and a recessed reset button (Figure D-2).

Figure D-2. CIU Front Panel LEDs

Table D-2 gives the meaning of each CIU LED.

Table D-2. CIU LED Meanings

LED	Description
Power	Flashes for 30 seconds while internal CIU diagnostics are being performed, and stays on while the CIU is operational. It continues flashing if power-on diagnostics detect a malfunction. Internal diagnostics should be completed in less than 90 seconds. If the Power LED keeps flashing after 90 seconds, call your Wang customer engineer.
Session Active	On when the CIU has one or more active sessions.

(continued)

Table D-2. CIU LED Meanings (continued)

LED	Description
Link Time Error	If the CIU transmitter is active longer than the maximum specified transmit time (3 milliseconds), this LED comes on and the transmitter automatically shuts off. To restart the transmitter, press and release the Link Error Reset button on the front panel. Once restarted, the transmitter tries to access Wang Band to allow normal communications to be reestablished without reinitializing the CIU. If the Link Timeout Error LED stays on after several tries, call your Wang customer engineer.

Side Panel LEDs

In addition to the front panel LEDs, a CIU has nine side panel (internal) LEDs that are used by Wang customer engineers. The leftmost LED (labeled F) indicates a memory parity error, if lit. The remaining LEDs are in a group of eight, labeled 1 through 8 from left to right. These LEDs are visible through the vent in the side panel of the CIU. They provide both diagnostic and normal activity information. Table D-3 gives the meaning of each LED.

Table D-3. CIU Diagnostic LEDs

LED	Indicates	Description
1	System activity	This LED is off if the CIU is in the idle state. If it appears to be on almost constantly, the CIU is heavily loaded.
2	Transmit	This LED comes on each time a message is transmitted to the network.
3	Receive	This LED comes on each time a message is received from the network.

(continued)

Table D-3. CIU Diagnostic LEDs (continued)

LED	Indicates	Description
4	Net enable	When this LED is on, the CIU is available to transmit or receive data over the network (CIU ready: DTR).
5	Host enable	When this LED is on, the CIU is available to exchange data with the system to which it is attached (DLP initialization completed).
6	Host receive	This LED comes on each time the CIU receives a message from the system to which it is attached.
7	Host transmit	The LED comes on each time the CIU sends a message to the system to which it is attached.
8	Hard error	If this LED is on, it indicates a CIU error, due either to a software or a hardware problem. In such cases, the meanings of the other seven LEDs change in relation to the problem. The system administrator must IPL the CIU after the problem is identified and corrected.

The meaning of each LED that is listed in Table D-3 changes if LED 8 is illuminated along with the other LED. Those changes are listed in Table D-4.

Table D-4. Changes to CIU Diagnostic LEDs

LED	Indicates	Description
1	Network transmit	Indicates a network transmit status error. Such an error may be due to a missing or broken drop cable or a failure in the main WangNet cable. Call your Wang customer engineer.
2	Unrecoverable interrupt	Indicates a hardware problem. Call your Wang customer engineer.
1 & 2	Data Terminal Ready dropped	Indicates a hardware problem. Call your Wang customer engineer.
3	Data Set Ready	Indicates a possible hardware problem. If dropped LEDs 8 and 3 are on, the Link Timeout LED on the front panel may also be on. Call your Wang customer engineer.
1 & 3	Duplicate cable address	Indicates a duplicate cable address. Another CIU on the network with the same address is active at the time your CIU is initialized. Check your configuration file to see if there is a remote system network address that is the same as your system's network address. If there is no duplication, an active system exists on the network that is not defined in your configuration file.

If one of the errors in Table D-4 occurs, the VS Operator's Console displays the message "Assistance required on device ##," and your system shuts down communications with the CIU.

MULTI-LINE TELECOMMUNICATIONS CONTROLLER LEDs

The following section gives the meaning of each LED on the Active Port Assembly (APA) panels connected to the Multi-Line Telecommunications Controller (MLTC) on VS 300 and 7000 Series systems. Figure D-3 illustrates the MLTC and the location of the LEDs on the APA panels.

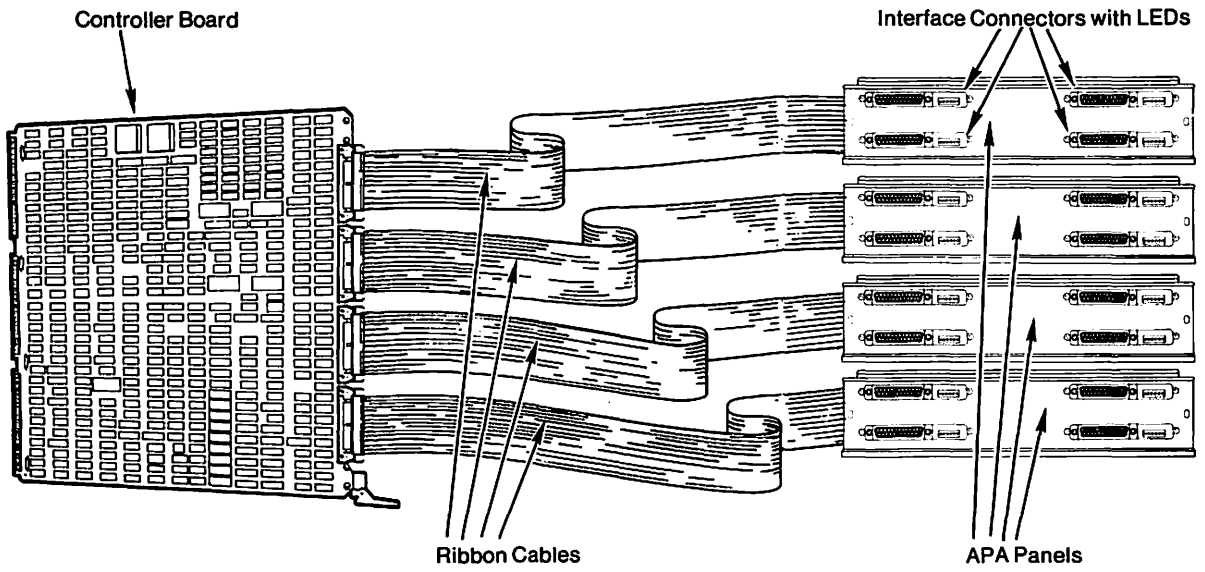

Figure D-3. 16-Port Model MLTC Components

Figure D-4 shows the LEDs as they appear on a single APA panel.

Data Set Ready	Data Term. Ready	Data Carrier Detect	Software Use	Transmit Data	Request To Send	Clear To Send	Receive Data

Figure D-4. APA Panel LEDS

Table D-5 presents the meaning of each APA panel LED.

Table D-5. APA Panel LEDs

LED	Indicates	Description
DSR	(Data Set Ready)	When on, this LED indicates that the data communications equipment (DCE) is connected to a communications line and is ready for data transmission.
DTR	(Data Terminal Ready)	When on, this LED indicates that the DTE has entered a telecommunicating mode and prepares the DCE for the establishment of a line connection. Both DTR and DSR must be on before data transmission can begin.[a]
DCD	(Data Carrier Detect)	When on, this LED indicates that a carrier wave has been detected from the remote DCE. This signal is sometimes referred to as the Received Line Signal Detector (RLSD).
BIT	(Built In Test)	When on, this LED indicates that MLTC diagnostic programs are being executed. This light will come on when you press the initialize button on the front panel.
TXD	(Transmit Data)	When on, this LED indicates that data is being transmitted to the remote system.
RTS	(Request To Send)	When on, this LED indicates that the DTE wants to enter transmit mode. The DCE should generate and send a carrier signal over the line in order to establish a link with the remote DCE (user data is not being transmitted at this time). When off, this LED indicates that the DTE has stopped transmitting data.
CTS	(Clear To Send)	When on, this LED indicates that the DCE is ready to transmit user data from the DTE. CTS is usually turned on a short time after RTS to allow the DCE transmit circuits to establish the carrier.

(continued)

Table D-5. APA Panel LEDs (continued)

LED	Indicates	Description
RXD	(Receive Data)	When on, this LED indicates that data or flags (hex 7Es) are being received from the remote system.

[a] DTE is the acronym for Data Terminal Equipment, which refers to the equipment installed on the inbound end of the RS-232-C (that is, the MLTC). The communications equipment on the outbound end of the RS-232-C interface (such as a modem) is referred to as the DCE, or Data Communications Equipment.

BASIC MODEM LEDs

The following section gives the meaning of each modem indicator light. Modems differ in the number of such lights that they have and in the labeling for the lights. (The labeling on your modem may differ from that presented in Table D-6.)

Table D-6. Basic Modem LEDs

LED	Indicates	Description
DTR	(Data Terminal Ready)	When on, this LED indicates that the DTE has entered a telecommunicating mode and prepares the modem for the establishment of a line connection. When off, the modem cannot become active. Both DTR and DSR must be on before data transmission can begin.[a]
DSR	(Data Set Ready)	When on, this LED indicates that the modem is connected to a communications line and is ready for data transmission. It also indicates that the modem is not in talk or dial mode. Both DTR and DSR must be on before data transmission can begin.

(continued)

Table D-6. Basic Modem LEDs (continued)

LED	Indicates	Description
RTS	(Request To Send)	When on, this LED indicates that the DTE wants to enter transmit mode. The modem should generate and send a carrier signal over the line in order to establish a link with the remote modem (user data is not being transmitted at this time). When off, this LED indicates that the DTE has stopped transmitting data.
RI	(Ring Indicator)	When on, this LED indicates that a ringing signal is being received. RI is typically used to initiate some form of automatic response from the DTE.
DCD	(Data Carrier Detect)	When on, this LED indicates that a carrier wave has been detected from the remote modem. This signal is sometimes referred to as the Received Line Signal Detector (RLSD).
CTS	(Clear To Send)	When on, this LED indicates that the modem is ready to transmit user data from the DTE. CTS is usually turned on a short time after RTS to allow the modem's transmit circuits to establish the carrier and to allow the receiver of the remote modem to synchronize with the carrier of the transmitting modem.
TXD	(Transmit Data)	When on, this LED indicates that data is being transmitted to the remote system.
RXD	(Receive Data)	When on, this LED indicates that data or flags (hex 7Es) are being received from the remote system.

[a] DTE is the acronym for Data Terminal Equipment, which refers to the equipment installed on the inbound end of the RS-232-C (that is, the TCB/DLP). The modem on the outbound end of the RS-232-C interface is referred to as the DCE, or Data Communications Equipment.

(continued)

COMMUNICATIONS SUSPENSION AND RESUMPTION

Network communications can be suspended for a number of reasons, such as transmission line problems or hardware failures. However, problems with the network should not affect the local operation of your system. If communications to or from your system are suspended or you cannot resume communications, check the Operator's Console for operator notification messages (refer to Appendix C), or try to work through the suggestions listed in Table D-7.

Table D-7. Communications Problems and Responses

Problem	Response
System can't load microcode to DLP.	1. Check the GENEDIT file to see how many device numbers are allocated to the DLP on the IOP. Check the active WSNEDIT file to ensure that the DLP name is correct and that the protocol for the link has been specified accurately. 2. Check the cable connectors between the DLP and the VS. Try another cable. Make sure that the system name you entered through the Manage Areas function of WSNEDIT matches the System WangNet ID defined during GENEDIT. 3. Check to see if the DLP power cord is plugged in and the unit is turned on. 4. Try another port on the IOP. If possible, try one that you know is working. This may necessitate a different WSNEDIT file to get the DLP name to match the port number. This action is a last resort, because it necessitates a re-IPL of the VS.
Assistance required by device ####.	1. If the device number indicated in the error message matches the lowest device number assigned to the CIU, there may be a duplicate address problem (check for lights on the side: 8, 1, and 3). Check with the network administrator for a system with the same address as the one you tried to use for your system.

(continued)

Table D-7. Communications Problems and Responses (continued)

Problem	Response
Assistance required by device ####.	2. If the DLP is a CIU, check the side LEDs. 3. This message may also mean that the DLP name in WSNEDIT is wrong. If it identifies the wrong IOP port, the microcode may have been loaded into the wrong device.
VS and DLP IPL, but there is no communication.	1. Press PF12 (Telecommunications), then PF6 (Communications Devices) to see that the lowest device number assigned to the DLP is labeled "Reserved and in use." If it is not labeled that way, a configuration error probably exists. Verify that the WangNet ID assigned in the GENEDIT file is defined in the directory file. 2. Press PF12 (Telecommunications), then PF3 (Communications Access) to see if communications are inhibited. 3. Press PF12 (Telecommunications), then PF4 (Communications Links) to see if communications are inhibited for the link.
The VS cannot communicate with a specific system but can communicate with other systems.	1. Call the remote system administrator to see if that system is running. Ask if your WangNet ID (as defined in GENEDIT) is the same as the name assigned to your system in the remote system's configuration file. 2. Check the active WSNEDIT file and the directory file. Is the remote system defined, and are its network name and address correct? 3. Check to see if the remote system can be reached in some other way. For example, if you cannot log on to the remote system, can you transfer files to that system? If so, check to see if either service is inhibited for each system.

(continued)

Table D-7. Communications Problems and Responses (continued)

Problem	Response
The VS cannot communicate with a specific system but can communicate with other systems.	4. Have the configuration files of either system been changed? Has either system been upgraded to a new software release? 5. Use the CNS Path Trace diagnostic tool (described in Chapter 5) if CNS is being used to communicate with the specific system.
Can't attach to another VS.	1. Check to see if there is any communication to the remote VS. Is the File Transfer service running between the two systems? If there is no communication at all, check the configuration files of both systems to see if the necessary addresses and IDs are correct. 2. See if any local user can attach to the remote VS. If so, either the ID and password are invalid, or no more virtual circuits to the remote VS are available. 3. Press PF12 (Telecommunications), then PF5 (Communications Systems) to see if the service has been inhibited to the remote VS. 4. Use the CNS Path Trace diagnostic tool (described in Chapter 5) if CNS is being used to communicate with the specific system.

(continued)

Table D-7. Communications Problems and Responses (continued)

Problem	Response
The File Transfer Manager cannot connect with a remote system.	1. If the remote system is a VS, is the File Transfer service inhibited to your system? 2. Are passwords specified at either system? If so, does the Send password of the remote system match the Receive password listed in your WSNEDIT file? Does the Receive password of the remote system match the Send password listed for your system in your WSNEDIT file? 3. Is the File Transfer Manager able to connect with any remote system? Are there circuits available? 4. Use the CNS Path Trace diagnostic tool (described in Chapter 5) if CNS is being used to communicate with the specific system. 5. Are there any other means of communicating with the remote system (RLOGON, @ATTACH@, CNS diagnostics, etc.)
Cannot find file or document sent to the local VS.	1. If the request was a retrieve request, check the retrieve queue for the status of the request. 2. Print or display the File Transfer log to see if the transfer took place. 3. Find out if a transfer group was used. If it was, check its default WP library (for documents), or default file, volume, and library names (for files). Check to see if a remote system group is associated with the remote system, and check its defaults. See if user override is allowed in the transfer group definition. If so, check with the sender to see what document ID or file, library, and volume were entered when the request was made.

PERIPHERALS BAND TROUBLESHOOTING

Table D-8 lists several possible Peripherals Band problems and possible responses to those problems.

Table D-8. Peripherals Band Problems and Responses

Problem	Response
Nothing works on a given channel.	1. Check to see if other channels are working. If none of the channels are working, the backbone signal levels probably need checking. Call your Wang customer engineer. 2. If the other channels are working, check the local ports and the channel setting on the CPU. If two CPUs are on the same channel, or if two WangNet IOPs in the same system are on the same channel, neither will function properly. Turn off one CPU and see if the other one functions properly. 3. Make sure that the numbered settings on the NETMUX or Ergo workstations correspond to the channel number listed in the GENEDIT file.
An Ergo workstation gets no response from its CIU.	1. Check to see if any other devices can communicate with the same CPU through the Peripherals Band. 2. Check the manufacturing ID and make sure the same ID is listed in the configuration. 3. Check that the channel number on the Ergo workstation matches the channel number on the CPU. 4. Try another user outlet, one that you know is working, or try another cable between the Ergo workstation and the user outlet.

(continued)

Table D-8. Peripherals Band Problems and Responses (continued)

Problem	Response
A device connected to a local port does not work	1. Check the configuration file to see if the port is included. If it is, check to see if the devices connected to the other ports are working. 2. Try to connect the device to another local port, one that you know is working. 3. Try another cable between the device and the IOP. 4. Check the configuration file to ensure that the correct type of device is configured.
NETMUX does not work.	1. Check the channel thumbwheel setting. If it matches the setting in GENEDIT, check to see if other NETMUXES or Ergo workstations on the channel are working. Make sure the CPU is functioning normally. 2. Check the manufacturing ID of the NETMUX. See if the ID matches the one listed in the configuration file. 3. Try a different user outlet, one that you know is working. Try a different cable between the NETMUX and the user outlet.
A NETMUX port does not work.	1. Check the configuration file to see if the port is configured. Check to see if the device type listed in the Description field is the correct type for the device connected to the NETMUX port. 2. If the port is configured properly, try a working device of the same type on the port. 3. Try the device on another port, one that you know is working. (Be sure that the Description field for that port indicates the type of device that you are checking.)

INDEX

D

E

V

W

X

WANG

Customer Comment Form

Publication Number 715-0164A

Title WSN VS NETWORK CONTROL AND MONITORING GUIDE

Help Us Help You . . .

We've worked hard to make this document useful, readable, and technically accurate. Did we succeed? Only you can tell us! Your comments and suggestions will help us improve our technical communications. Please take a few minutes to let us know how you feel.

How did you receive this publication?

- ☐ Support or Sales Rep
- ☐ Wang Supplies Division
- ☐ From another user
- ☐ Enclosed with equipment
- ☐ Don't know
- ☐ Other _____

How did you use this Publication?

- ☐ Introduction to the subject
- ☐ Classroom text (student)
- ☐ Classroom text (teacher)
- ☐ Self-study text
- ☐ Aid to advanced knowledge
- ☐ Guide to operating instructions
- ☐ As a reference manual
- ☐ Other _____

Please rate the quality of this publication in each of the following areas.

	EXCELLENT	GOOD	FAIR	POOR	VERY POOR
Technical Accuracy — Does the system work the way the manual says it does?	☐	☐	☐	☐	☐
Readability — Is the manual easy to read and understand?	☐	☐	☐	☐	☐
Clarity — Are the instructions easy to follow?	☐	☐	☐	☐	☐
Examples — Were they helpful, realistic? Were there enough of them?	☐	☐	☐	☐	☐
Organization — Was it logical? Was it easy to find what you needed to know?	☐	☐	☐	☐	☐
Illustrations — Were they clear and useful?	☐	☐	☐	☐	☐
Physical Attractiveness — What did you think of the printing, binding, etc?	☐	☐	☐	☐	☐

Were there any terms or concepts that were not defined properly? ☐ Y ☐ N If so, what were they? _____

After reading this document do you feel that you will be able to operate the equipment/software? ☐ Yes ☐ No ☐ Yes, with practice

What errors or faults did you find in the manual? (Please include page numbers) _____

Do you have any other comments or suggestions? _____

Name _____ **Street** _____

Title _____ **City** _____

Dept/Mail Stop _____ **State/Country** _____

Company _____ **Zip Code** _____ **Telephone** _____

Thank you for your help.

Printed in U.S.A. 14-3140A 2-88

WANG

Cut along dotted line

Fold

NO POSTAGE
NECESSARY IF
MAILED IN THE
UNITED STATES

WANG

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 16 LOWELL, MA

POSTAGE WILL BE PAID BY ADDRESSEE

Wang Laboratories, Inc.
Technical Publications Dept.
M/S 012-260
One Industrial Avenue
Lowell, Massachusetts 01851-9971

Fold

WANG

To Order by Phone, Call:
1-(800)225-0234
Telex 172108

Order Form for Wang Manuals and Documentation

① Customer Number (If Known)

② Bill To: Ship To:

③ Customer Contact: ( ) ( ) ④ Date Purchase Order Number
Phone Name

⑤ Taxable Yes ☐ No ☐ ⑥ Tax Exempt Number ⑦ Credit This Order to A Wang Salesperson Please Complete Salesperson's Name Employee No. RDB No.

⑧ Document Number	Description	Quantity	⑨ Unit Price	Total Price

⑩ Authorized Signature Date

Sub Total	
Less Any Applicable Discount	
Sub Total	
LocalStateTax	
Total Amount	

☐ Check this box if you would like a free copy of
WangDirect Software & Literature Catalog
(711-0888A)

Ordering Instructions

1. If you have purchased supplies from Wang before, and know your Customer Number, please write it here.
2. Provide appropriate Billing Address and Shipping Address.
3. Please provide a phone number and name, should it be necessary for WANG to contact you about your order.
4. Your purchase order number and date.
5. Show whether order is taxable or not.
6. If tax exempt, please provide your exemption number.
7. If you wish credit for this order to be given to a WANG salesperson, please complete.
8. Show part numbers, description and quantity for each product ordered.
9. *Pricing extensions and totaling can be completed at your option; Wang will refigure these prices and add freight on your invoice.*
10. Signature of authorized buyer and date.

Wang Terms and Conditions

1. **TAXES** — Prices are exclusive of all sales, use, and like taxes.
2. **DELIVERY** — Delivery will be F.O.B. Wang's plant. Customer will be billed for freight charges; and unless customer specifies otherwise, all shipments will go best way surface as determined by Wang. Wang shall not assume any liability in connection with the shipment nor shall the carrier be construed to be an agent of Wang. If the customer requests that Wang arrange for insurance the customer will be billed for the insurance charges.
3. **PAYMENT** — Terms are net 30 days from date of invoice. Unless otherwise stated by customer, partial shipments will generate partial invoices.
4. **PRICES** — The prices shown are subject to change without notice. Individual document prices may be found in the WangDirect Software & Literature Catalog (711-0888A)
5. **LIMITATION OF LIABILITY** — In no event shall Wang be liable for loss of data or for special, incidental or consequential damages in connection with or arising out of the use of or information contained in any manuals or documentation furnished hereunder.

Printed in U.S.A. 14-3141A 2-88

WANG

Cut along dotted line

Fold

NO POSTAGE
NECESSARY IF
MAILED IN THE
UNITED STATES

WANG

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 16 LOWELL, MA

POSTAGE WILL BE PAID BY ADDRESSEE

WangDirect
Wang Laboratories, Inc.
M/S 017-110
800 Chelmsford Street
Lowell, Massachusetts 01851-9972

Fold

WANG

ONE INDUSTRIAL AVENUE, LOWELL, MA 01851
TEL: (508) 459-5000, TELEX 172108

Printed in U.S.A. 715-0164A 7-88